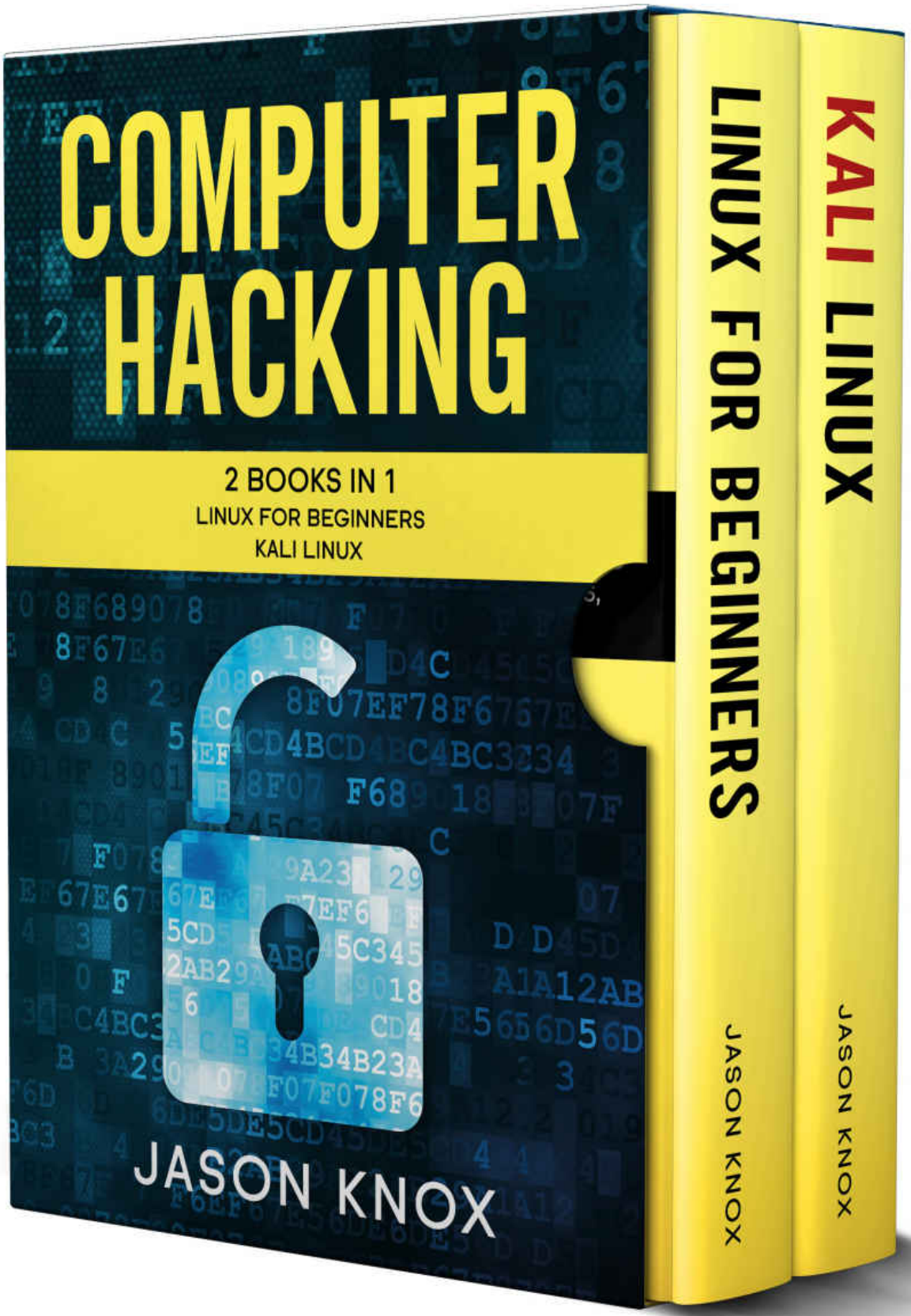

COMPUTER HACKING
2 BOOKS IN 1
LINUX FOR BEGINNERS
KALI LINUX
JASON KNOX
LINUX FOR BEGINNERS
JASON KNOX
KALI LINUX
JASON KNOX

Computer Hacking

2 Books in 1:

Linux for Beginners
Kali Linux

Jason Knox

1. Linux for Beginners

2. Kali Linux

Linux for Beginners

An Introduction to Linux Programming Basics for Hackers, Its Operating System, Command-Line and Networking, Including Effective Strategies, Tips and Tricks to Learn How It Works

Table of Contents

Introduction
Chapter 1: What is the Linux Operating System?
- What is Linux?
- Why Should I Use Linux?
- Open Sourced
- What is a Distribution?
- Which Distribution Is Best?

Chapter 2: How to Install Virtual Machines?
Chapter 3: Understanding the Directory Structure of Linux
Chapter 4: The Commands You Need to Know in Linux
- The Listing Directories and Files
- Making Some Directories
- Changing Your Location to a New Directory
- The Pathnames
- Copying the Files
- Removing a File or a Directory
- How to Display File Contents on the Screen
- How to Look Through the Contents of a File
- Appending Files
- The Help Command

Chapter 5: Teach Yourself to Fish
- Learning Fish
- Running Some Commands in Fish
- The Variables
- The Lists
- The Command Substitutions
- Functions
- $PATH

Chapter 6: How to Handle Your Editors
- Nano
- Working with Vi

Chapter 7: The Necessary Permissions

Viewing Permissions
Changing the Permissions
Shorthand to Set the Permissions
Basic Security to Follow
Chapter 8: Looking at the Variables of Your Environment
Utilities
How to Define the Variable
More to Learn Here
Chapter 9: Linux and Hacking
Conclusion

Introduction

Congratulations on purchasing *Linux for Beginners:An Introduction to Linux Programming Basics for Hackers, Its Operating System, Command-Line and Networking, Including Effective Strategies, Tips and Tricks to Learn How It Works,* and thank you for doing so.

The following chapters will discuss all of the things that you need to know in order to get started with the Linux operating system. There are a lot of options out there for operating systems, but most of us are going to focus our attention on how to work with options like Mac and Windows. But while those are the most common options out there to work with, many people are starting to see the benefits of working with Linux. This operating system is more secure, easier to work with, and can provide us with the power that we need to get a lot of things done in the process. This guidebook is going to spend some time looking at how this will work for our needs, as well.

Inside this guidebook, we are going to take a look at the Linux system and how we are able to use this for some of our own needs as well. We will start out with a look at some of the neat things that come with Linux, the benefits of working with this one compared to some of the other options. This will help us to see what this is one of the best options to work with and will ensure that we are going to be able to get all of the benefits that we are looking for in no time at all.

Then it is time to move on to some of the things that we are able to do when we are working on the Linux system as well. We will explore first how to set up our own virtual box, and how this helps us to work with the Linux operating system, without getting rid of the traditional operating system found on our computers. While you can choose to just switch completely over to the Linux operating system if you would like many programmers are more comfortable with having this as an add-on and then working with their traditional operating system as well. This is what the VirtualBox can help us to accomplish.

We are also able to move on to some of the commands that are going to be so prevalent when we handle some of our work with Linux. We will spend a good deal of time looking at the basics of Linux and how we are able to use these commands to get a lot of things done in a short amount of time, as well. These commands will help us to create some of the files that we need, change them, and so much more, which can make the Linux system easier to use overall.

This is just a start to what we are going to look at when it is time to work with this guidebook and all of the neat things that are possible with the

Linux operating system. We will look at how we can grant the right permissions to get this to work the way that we would like, how to handle some of the different shells that are present, and even a look at how to use the Fish shell. There are a lot of other options in shells that we are able to explore when it comes to using this kind of operating system. But when it comes to the ease of use that we are going to see, and all of the power that comes with it, you will find that Fish is one of the best options to choose from.

In addition, we are going to take a look at how to keep the security of your system intact, how to pick out the right text editor, along with some of the basics of using some of the most common text editors that we are able to focus on. And then, we will end the guidebook with a look at how the Linux system is able to work along with some of the hacking that you may want to practice to keep your system safe. There are a lot of reasons to work with Linux, but many people choose to work with this because it allows them to learn some of the basics of hacking in an easy and efficient manner.

There are a lot of great things that we are able to work with the Linux operating system, especially when it is compared to some of the other operating systems that are out there. But it is still not one that many people are familiar with, and that causes them to miss out on it quite a bit. With this in mind, make sure to check out this guidebook and learn a bit more about how the Linux operating system can work for your needs.

There are plenty of books on this subject on the market, thanks again for choosing this one! Every effort was made to ensure it is full of as much useful information as possible; please enjoy it!

Chapter 1: What is the Linux Operating System?

Before we are able to get into some of the cool codes and more that we are able to do with the Linux system, we first need to take a look at what Linux is. While this may not quite have the name recognition that we are going to find with some of the other operating systems out there, like Mac and Windows, you will find that Linux is creating its own niche and becoming more popular each day. That is why we need to spend some time learning more about this and what we are able to do with it overall.

From cars to smartphones, home applications and supercomputers, enterprise servers to home desktops, this operating system is going to be all around us. This is a newer operating system in some respects, and it came out around the mid-1990s. Since that time, it has been able to reach a big user-base that is found throughout the globe. In fact, we are going to find that Linux is found, in one form or another, all around us.

Linux is really versatile and a great option to work with, so you will find that it is going to be inside a lot of the options that you use on a regular basis. For example, many phones are going to have Linux inside of them. In addition, it is going to be found in thermostats, in cars, Roku devices, televisions, cars and so much more. And it is also responsible for running much of what we are able to find on the Internet, so that is a big plus as well.

But, outside of being one of the platforms of choice to help out with a lot of the work that needs to be done with embedded systems, servers and even desktops that are found throughout the world, Linux is actually going to have a lot of benefits that we are able to rely on as well. For example, when it is compared to some of the other operating systems that are out there, it is one of the most reliable, worry-free and secure options that you are able to choose.

With some of this in mind, it is time for us to go through and learn a bit more about some of the parts that come with this operating system, and how we are able to use these for our own benefit as well. Here is all of the information that you need to know as someone who is new to the Linux platform.

What is Linux?

The first thing that we need to take a look at is the fact that Linux is going to be an operating system. It is similar to the operating systems that we use like Mac OS, iOS and Windows. In fact, one of the most popular platforms that is found on the planet, Android, is going to be powered thanks to the Linux operating system.

To break this down, the operating system is simply going to be a type of software that is going to be able to manage all of the resources of the hardware that are associated with your laptop or desktop. To keep it simple, the operating system is going to help manage all of the communication that happens between the hardware and the software. If you did not have an operating system in place, then the software would not be able to function the way that you would like.

You will find that, just like some of the other operating systems that are out there, the Linux operating system is going to come in with a few different pieces that we need to work with. Some of these are going to include:

1. Bootloader: This is going to be the software that is able to manage the boot process on our computer. For most users, this is going to just be the splash screen that is going to pop up and then will go away when you are first booting up into the operating system.
2. Kernel: This is going to be the one piece of the whole that is called Linux. This is going to be the core of our system and it is responsible for managing the memory peripheral devices and CPU. The kernel is going to be the bottom level that we will find with our operating system.
3. Init system: This is going to be one of the sub-systems that are going to bootstrap the user space, and then it will be in control of the daemons. One of the most widely used of these is going to be a system, which is also sometimes seen as the most controversial of them. This is going to be the system that is responsible for booting up the operating system, once the initial booting is handed over from the initial bootloader that we use.
4. Daemons: These are going to be some of the background services. It could include options like scheduling, sound and printing, but you can move them around to fit your needs. They are either going to start up when you do a boot of the system, or after you have had a chance to log into the desktop.
5. Graphical server: This is going to be the sub-system that will display all of the different graphics that you want on the monitor. It is going to

be referred to as X or the x server.

6. Desktop environment: This is going to be the piece of the operating system that you are actually going to spend time interacting with. There are going to be a lot of options for this kind of environment that we are able to choose from, including Cinnamon, Pantheon Enlightenment and more. Each of these environments is going to include some of the applications that you need built-in, including the games, web browsers, configuration tools, file managers and more.
7. Applications: The desktop environment that you choose is not going to come with a ton of applications for you to choose from. Instead, it is going to be necessary for you to go out and search for the software titles that you want, and then you can find them and install them for your needs. For example, Ubuntu Linux is going to have what is known as the Ubuntu Software Center, which is going to help you go through thousands of apps, and then install the ones that you like the most, from one centralized location.

Why Should I Use Linux?

This is one of the first questions that a lot of people are going to ask when they first hear about the Linux system overall. They may be curious as to why they should learn a completely new computing environment when the operating system that is already on their computer and was shipped to them when they ordered the device is working just fine. Would it really be worth their time to learn a new one and see how it works?

To help us to answer this question, it is important to answer a few other questions to give us a good idea of what the Linux system can do for us that our traditional operating system is not able to do. For example, does the

operating system that you are currently using actually work just fine? Or are you constantly dealing with a lot of obstacles like malware, viruses, slowdowns, costly repairs, licensing fees and crashes all of the time?

If you find that these are things that you are dealing with on a regular basis, especially once you have had the computer for some time, then you may find that the perfect platform for you to use to prevent some of this is going to be the Linux system. It is one of the operating systems that has evolved to become one of the most reliable out of all of them. And when you are able to combine all of that reliability with zero costs, you will end up with the perfect solution for the platform that you need.

That is right, you are able to get the Linux system and all of the benefits that come with it all together for free. And you are able to take the Linux operating system and install it on as many computers as you would like, and use it as much as you would like, without having to worry about how much it will cost to use, how much the software is, and you also don't need to worry about server licensing.

We can also take a look at the cost of adding on a server in Linux compared to the Windows Server 2016. The price of the Windows option for a standard edition is going to be about $882 if you purchase it right from Microsoft and not from another part. This is not going to include any of the Client Access Licenses, and the licenses for all of the other software that you decide are important and need to be run in this as well, such as a mail server, web server and a database.

For example, the single user who works with the CAL on the Windows system is going to cost you about $38. But if you need to have a lot of users, that cost is going to go up pretty quickly. If you need to work with ten people on the server, then you are going to end up with $380 just to do that part. And that is just with the software licensing that you would like to get done.

But it is a bit different when we are working with the Linux server. For the Linux option, you will be able to get all of that for free and it is also easy for you to install. In fact, being able to go through and add in a web server with all of the features, including a database server, is just going to take a few clicks or a few commands to get done.

This alone, especially for some of the bigger businesses out there, will be enough to win others over to this operating system. But there are a few other benefits that are going to show up as well. This operating system is going to work and keep out the troubles, for as long as you choose to work with it. And it is often able to fight off issues of ransomware and malware and even viruses better than some of the others. And you will not need to reboot this all that often unless the kernel has to be updated, and this is often only done every few years.

If you have ever been frustrated with the operating system that you are working with and how it may not always do what you would like, that means it may be time for you to work with the Linux operating system. It is going to have all of the benefits that we want and will also be free to use, no matter how many computers you decide to hook it up to along the way.

Open Sourced

Another thing that we are going to enjoy when it is time to work with the Linux system is that it is open-sourced. This means that it is going to be distributed under this source license so that you are able to work with it in the manner that you would like. Open source is going to be useful for a number of reasons, but we will find that there are a few key tenants that we need to focus on, include:

1. You will find that you have the freedom to run the program, no matter what the purpose is.
2. You will find that you have the freedom to study and learn more about how this program works and what you can make any of the changes to it that you wish along the way.
3. You have the freedom to redistribute copies so that you are able to use it more than once for your own needs or to provide it to your neighbor who would like to use it as well.
4. You will find that you have the freedom to make some modifications to it in the manner that you would like, and then you can also distribute copies of these modifications to others.

There are going to be crucial points to understand when it comes to working with the Linux system and understanding more about the community that is going to work to create this kind of platform in the first place. Without a double, this is going to be an operating system that is by the people and for the people. These tenants are also going to be a big factor in why people are going to choose to work with this kind of operating system compared to some of the others. It is all about freedom, and freedom of use, and the freedom of choice, and the freedom to not have to worry about a bunch of crazy rules and other issues along the way.

What is a Distribution?

The next thing that we need to take some time to look at is the distribution part that comes with Linux. Linux is going to come with a number of versions that are going to suit the type of user you would like. Whether you are someone who is brand new to working with this or you have worked with programming and other similar things for a long time, you are sure to find the type of Linux that is going to be able to match all of your needs that you would like.

All of the versions that are available for Linux are going to be known as the distributions. And nearly all of these distributions that come from Linux are ones that we are able to download for free, burn over to a disk or a USB drive and install on as many different devices that we would like.

There are a ton of distributions of Linux that are popular, and it is often going to depend on what you are hoping to do with the operating system in the first place. For example, you could find Kali Linux, LINUX MINT, MANJARO, OpenSUSE, ELEMENTARY OS, SOLUS, FEDORA, ANTERGOS, UBUNTU and DEBIAN. And there are a lot of other options based on your own personal preferences along the way as well.

You will find that each of the distributions above is going to come with a different take on what the desktop should be doing during this time. Some are going to opt for some modern user interfaces, and these would include options like GNOME and Elementary OS. And then there are a few that are going to stick with a desktop environment that is more traditional and maybe closer to what we are working with in the past.

Of course, this doesn't mean that we need to leave the server behind here. For this arena, we have a lot of options like the SUSE Enterprise Linux, Centos, Ubuntu Server and Red Hat Enterprise Linux.

Now, some of the server distributions that we talked about above are going to be free. This may include the CentOS or the Ubuntu Server. And then there are going to be the other two that have a price with those. The main difference is that the ones that cost a bit are going to provide some support, so if this is important to you, then you should consider the pricing and go with those as well. You can get a lot of benefits out of Ubuntu and the free options as well, so do your research and figure out which one is going to meet your needs the best.

Which Distribution Is Best?

Before we end this, though, we need to take a look at which distribution is going to be the best. There are a lot of great ones out there that we are able to work with depending on what matters the most for our needs. And sometimes it is going to be based on the skills that we have, what we would like to do with this process and more. Some of the things that we need to consider when it is time to pick a distribution to work with will include:

1. How skilled are you at using the computer and working with some command-line interfaces rather than the graphical interface?

2. Do you find that you prefer a standard or a modern desktop interface?
3. Would you rather work with a desktop or a server?

If you would rather not work with anything that is too complicated when it comes to your computer skills, then you would want to pick out one of the distributions that are present that are meant to work well for newbies of Linux. Ubuntu, Linux Mint and Elementary OS are great options to work with. If you find that your skills in using the computer extend into the above-average range, then there are a few others that offer some more skills and features, including Fedora and Debian.

Of course, if you are someone who has spent a lot of time on computers and have been able to spend quite a bit of your time working on these along the way, then you can take it up to the next level. The best distribution for this is going to be Gentoo. And if you would really like to have some kind of challenge, you are able to go through and build up your own distribution of Linux and often working with Linux from scratch is a good option.

If you want to make sure that you are working with a server-only distribution option, you will need to decide if you would like to work the command line only option or if you would like to stay with the desktop interface. The Ubuntu Server, for example, is not going to install that GUI interface, so if that is something that you want to work with, then you will need to pick another distribution to make things work.

When you are working without the GUI interface, for example, then that means that you are not going to be bogged down with all of the graphics that need to load up when you are starting the server. But keep in mind that

you have to work with the command line in Linux so that you can get into the parts of the system that you want. If you are not good with the command line or doing some of the codings that go with this, then you may want to consider going with another option as well.

The nice thing, though, is that if you would like to work with the Ubuntu Server, but you would also like to have the graphical parts there, then there is a GUI package that you are able to install to make it work for any programming that you would like. System administrators will also want to view a distribution while looking at some of the features that are going to come with it to ensure they are able to do some of the actions that they would like.

For example, would you like to work with a server-specific distribution that will offer you, right out of the box, all of the different features and parts that you need for your server? If this is something that sounds good for you, then you may want to go with an option like CentOS. Or, would it be better for you to work with a desktop distribution and then add in the pieces that you need as time goes on? If this is something that sounds more appealing to you, then Ubuntu or Debian may be better choices to go with.

As we can see, there are a lot of different parts that we are able to work with along the way when it comes to working on the Linux system. You will find that there are many ways that Linux is already being used in the world, even if we didn't realize it as much in the beginning. And we are able to take this and utilize it for some of our own needs with the help of adding this operating system to our computers and using it on a daily basis, or to help out with things like coding and hacking as we need. When you are ready to

learn more about this great operating system, make sure to check out the rest of this guidebook to get started.

Chapter 2: How to Install Virtual Machines?

The next thing that we need to talk about is the use of a VirtualBox on our system to make sure that we can handle some of the work that we need to finish with Linux. VirtualBox is going to be one of the virtual machines that, first developed by the company of Sun Microsystems, is now under the ownership of Oracle. It is able to stimulate a separate computer and each virtual machine is going to come with its own operating system, applications and a lot of other things that you need to do for the coding.

VirtualBox is going to be a good option to work with when you would like to test out a lot of operating systems. For our needs, we are going to use it in order to add the Linux operating system on a Mac OS or Windows operating system. By using the Linux operating system in this manner, you don't need to make any permanent changes to the system that you are currently using. This makes it easier to use Linux just when you want to, and then switch over to one of the other options if that is what you would like to do.

Keep in mind you do have the option of using Linux as the main operating system on your computer if you would like. You can go through and take the other operating system off your computer if that works the best for your needs and can help you get things done. But many times, people want to work with Linux for some specific needs, so they will want to work with

the VirtualBox to make this happen while keeping their traditional operating system in place.

With this in mind, we are going to spend some time looking at how we are able to install this VirtualBox program on our Windows or Mac system along the way. We are going to start out with installing it on our Windows system:

1. Go to the download page for VirtualBox and then look for the latest version that has been released at the time you visit. Click on this link.
2. When you are redirected to the next page, you want to look specifically for the file that is going to end in .exe and then download this. Pay attention to the location where you save this on your computer so that you can find it later on.
3. Once the installer has gone through the downloading process, you can go and find the .exe file and double-click on it. You can then follow the instructions on the screen in order to install this onto Windows. Keep in mind that when you are doing this that you may end up losing some of the network connections during this time because the virtual network adapters are being installed.
4. Now you need to go through the process of rebooting your computer. And when you do this, you will be able to find the VirtualBox in your own apps to use. From here, we are able to run this and install any of the other operating systems of our choice.

That is all that we need to do in order to get this whole program downloaded on our Windows system. But we are also able to do a similar

process when it is time to work with doing this on a Mac operating system. The steps that we need to use to get this to happen includes:

1. Go to the download page for VirtualBox and then download the latest version of this app for the Mac.
2. Save the .dmg to a file location that you will easily be able to remember. You also want to make sure that you download the OS X hosts version.
3. When this download is done, you will want to locate the file and then install it with the help of the executable file.
4. When all of this is done, you are able to reboot your computer, and then it is time to use the VirtualBox.

Another thing that we are able to work with is how we can install this Linux operating system with the help of an image for VirtualBox. There are a few steps that we are able to use in order to get this to work in the manner that we would like. Again, we are going to work with the Windows system. After you have gone through the other steps that we did in the last part for downloading VirtualBox on Windows, it is time to work with downloading the disk image for Ubuntu Linux including:

1. First, if you do not have the BitTorrent client installed on your computer, you should take some time to install this right now. BitTorrent is going to be a P2P application that is going to allow us to have downloads from other users, which is going to really ease the loading that happens on the Ubuntu servers.
2. Now head to the Ubuntu release website and then make sure that you click on the latest release version to download it. You do not want to

click on any of the links for a Desktop CD. You will find a full list of links that are at the bottom of this page, but you want to make sure to click on the one with the .iso.torrent extension. Download this somewhere that you are going to remember later on.

3. Then we can copy this to a bootable USB that we are able to use for our needs.

Something that we need to keep in mind here is that if you are working with an installation of WinRAR, it is going to automatically associate itself with the file that you downloaded and will ask if you would like to use this to help extract the contents. You DO NOT want to use this to extract the file, so don't do this.

Before we move on to the other steps that we need to use here, you need to make sure that we back up the contents of our hard drive somewhere that is safe. It is highly likely that you are going to lose everything if you do not go through and do this step. Then the other steps that we need to work with on this system will include:

1. You will want to open up the VirtualBox from the start menu before clicking on New. This is going to help us to open up the New Virtual Machine Wizard.
2. Click on Next and then provide a name for this virtual machine. Calling it something easy to remember is usually the best bet.
3. If you end up having more than 1 GB of RAM available to use on your computer, allocate one-quarter maximum to the machine that we are making. If you have less, then you will need to stick with the recommendations of VirtualBox here. Then click on Next.

4. When you are read, you will want to click on Create New Hard Disk before clicking on Next.
5. Click on Next another time and you will end up on a screen where you are able to set up the type of hard drive that you would like to use. Our goal here is to choose Fixed-Size Storage.
6. If you intend to add in some software or you would like to install some really large files in this, then you will want to make sure there is some buffer here. Then click on Create.
7. Once we have been able to create the virtual hard drive, you will then need to add in the .iso image that we downloaded earlier. You can do this by clicking on Settings, then Storage and then on CD/DVD device.
8. Where there is the word Empty, there should be a folder icon that we are able to click on.
9. Choose the .iso that we went through and downloaded it already and then click on OK from here.
10. Now you can double-click on the virtual machine to get it to start up the way that you would like.
11. You will then be able to get a lot of instructions and warnings about using the guest operating system. You should take some time to read them and then mark them up so that they won't show up and interrupt again.
12. Give the system a bit of time to load up Ubuntu.
13. Before you are able to install Linux all of the ways, you first need to change up the BIOS settings on your computer. Usually, when you get the computer to start up, you will it the F1, F2, F12, Escape or Delete. You can restart your computer now and get into the

BIOS settings and change up the boot option so that you boot from USB first.

14. Now it is time to plug the USB stick into the computer and do a reboot of the system again.
15. This is where we are going to see a screen that is blank, except for a few smaller logos on the bottom. Press on any key and a new screen is going to show up. Make sure to choose the language that you would like to work with.
16. Now we can click to Install Ubuntu. This is going to get the installer to start. Depending on the version, you may be asked to choose the language again.
17. This is where we will tick on the option so that we install the closed-source software as well.
18. Now you are going to be asked to connect back onto the Wi-Fi if this is not automatically done for you. You do not need to do this, and it honestly slows down the process that you are doing, so skip it for now so that you can get it done.
19. This is where we are going to see three options. We want to click on the first one and then drag the slider to choose the sizes of the hard drive for both of these. This is going to help our drive be partitioned into two parts.
20. Then there will be a few questions that will show up on your screen. You can answer them to fit your needs.
21. Now we just need to wait a few minutes for Ubuntu to be installed, depending on the speed of your computer. This can sometimes take an hour to get it all done.
22. When this is done, you will need to reboot your computer and take the USB stick out of it. When you boot the computer up again,

you should be in the Ubuntu environment as you would like.

If you went through and changed up the size of the partition that you were working within Windows, you are going to be asked to work on a disk check. This is not something that is necessary to work with, though. If you would like to do it, though, you can go back to Settings, then Storage and then CD/DVD and check that the entry is Empty again. This is going to help us out because it is going to eliminate any need for us to use the USB each time that we would boot up our computer.

From there, we are able to work with the Mac operating system and how we are able to go through this process as well. When you have finished up with the installation of the VirtualBox, it is time to download the iso to make this all work the way that we would like. The steps that we are able to use to make this happen includes:

1. First, we need to head to the download page and then click on the iso image for Mac. You will also want to choose your geographical location and then click on Begin Download. You want to make sure that you are saving the file rather than opening or mounting it.
2. When you get to this point, you will want to open up the VirtualBox and register it.
3. Now you are able to click on creating a new virtual machine. You can click on New to open up the wizard that you would like to work with, as well. Click on Next and then type in the name that you would like to use for this virtual machine.
4. When you are asked, you will want to choose the Linux Ubuntu option for the operating system before licking on Net. Set the base

memory as 384 MB and then click on Next.

5. When we are at this point, we need to click in order to create a new hard disk. This is going to be a disk that is going to take up some space on your existing drive. You need to make sure that there is enough memory for you to do this. Accept the default settings that are there and then click on Next.
6. At this time, the Create New Virtual Disk wizard is going to appear and you will want to click on the Next button. And then click on Dynamically Expanding Storage before clicking on Next again.
7. This is where we are going to choose where we would like to place the hard drive and how big we would like to have it. 2 TB is the maximum here, but for the most part, 8 GB will be enough. Click on Next when you are done with this and then on Finish.
8. When you get here, the framework is going to be ready, so you need to make sure that you have copied the iso to the bootable USB or DVD disk. Insert your USB or DVD. You can click on the CD/DVD and then tick for it to Mount this drive.
9. Click on your ISO Image File. Click on the folder beside the No Media and then drag your iso file onto it before clicking on Select and then on OK.
10. Click on Start, and then you will see a black screen show up. This is going to be the new session and everything you do now is going to happen on the virtual machine. If you would like to be able to change things back to Mac, you just have to click on the Command key on the left side of the space bar. Click OK.
11. When the Ubuntu screen shows up, you can double click to Install and then answer any of the questions that show up on the

screen. When this is done, click on Forward and accept the default values that are there to make it easier before clicking on Forward.

12. Here we are able to input some of our own personal information, including a new password and a name for the machine. You can also choose whether you would like to have this log in automatically or if you would like to have it protected by a password and then click on Forward.
13. Click on Install and then wait for a bit to give it time to load up.
14. When this installation is done, you will either be sent into it automatically, or you will need to use the password that you set up. This all depends on the way that you set it up in the beginning.
15. Ubuntu is going to spend some time checking for updates, so make sure to click on Install Updates and wait a few minutes. Then Reboot the Mac, and you are all ready to get things done.

Chapter 3: Understanding the Directory Structure of Linux

Now that we have more knowledge about how Linux is going to work and some of the steps that we need to take in order to set up the VirtualBox so we can get our own work done, it is time to take a look at some of the different parts of the directory of Linux. If you are planning on working with the Linux system and all that it has to offer, then we need to make sure that we understand some of the structure that comes with the directory of Linux.

If you are moving over to Linux from the Windows system, then you may find this directory a bit strange. There are also not going to be the drive letters because these will be replaced with other options. The FHS, or the File Hierarchy System, is going to define the file system structure when we are on Linux, but there are going to be a few other directories that have not been given their definition with this standard.

The first one is going to be the root directory. We are able to signify this with the (/) symbol. When you work with Linux, everything is going to be found under this directory, which is known as the root directory. This is going to be similar to what we find with C:/ in the Windows system, but there won't be the drive letters when you work with this.

Then we can go on to the /bin directory. This one is going to be known as the essential user binaries. This is a directory that is home to the programs or binaries that are going to be essential to the system being mounted in single-user mode. You would find that something like FireFox is going to be stored in the directory that is known as /usr/bin while some of the other system programs and utilities, like the bash shell, are going to be found in /bin. /

The /boot is going to be known as the static boot files. This is where the files that are needed to help make sure the system we are booting up will be found here. This could be the GRUB boot loader and the kernel files. The configuration files that you want to work with are going to be found in /etc. which will talk about further on in this guidebook.

Next on this list is going to be the /cdrom, which is the Mount Point for the CD-ROMs. This is a directory that we are not going to find under the standard of FHS but is still to be found in most of the operating systems. It is a temporary location for when you insert a CD-ROM into your computer.

/dev is the next option on the board, and this is going to be for the device files. Devices are going to be the exposed files that are on Linux, and this particular directory is going to come with several special files that are going to be representative of devices. These are not going to be the same kinds of files that we are used to working with, but they will look similar. For example, if you see the /dev/sda, it is going to be there to represent the initial SATA drive in your system. You will also find that there are a few pseudo devices that will come up here, which are basically going to be

some virtual devices that are not going to hook up to any hardware in the process.

We talked about this one a bit before, but it is going to be the /etc. configuration files that we can use. This is where you will want to search when you are looking for your configuration files, and you will be able to do some editing with these on any text editor. However, we have to remember that only the configurations of the system are going to be found on this one. If you are going with some that are more user-specific, then you need to search for these on the home directory of the user.

The home folders or /home is where we are able to find the home folder for all of the users that we are working with. This is going to contain some of the data files, as well as the configuration files that are specific to the users on the system, and then each of the users will be the only ones who can write in these home folders. If you would like to make some modifications to the others, then you will need to become the root user so that you have the elevated permissions.

We can also work with the /lib directory, which is going to be the essential shared libraries. This is going to contain all of the libraries that the binaries are found in the /sbin and .bin need to work well.

Some of the other directories that we need to spend some time on when handling this kind of process will include:

1. /lost+found: These are going to be all of the files that are recovered. All of the file systems that you work with will have this kind of

directory. If there is some reason that your system is going to crash, when you boot up again, a file system check will be done. If these corrupted files are found, they will be placed into this directory so that you are able to find them when needed for later.

2. /media: This is going to be the removable media. Here we are going to find all of the subdirectories, and this is also where some of the removable media is going to be mounted. For example, this will be where we find the USB, DVD or BD is going to be found. When each of these is mounted, you will find a new drive appearing, which allows us to access the media contents.
3. /mnt: This one is the temporary mount point. This is the place where the administrators are going to mount the temp file systems when they are in the process of using it.
4. /opt: This one is going to be for the optional packages. Here we are going to be able to find some of the subdirectories for the software packages that you can optionally choose to work with. It is generally going to be used by the software that you are working with, but which is not going to follow the rules of the standard FSH.
5. /proc: This is going to be the Kernel and Process Files. This is going to be similar to what we find with the /dev directory because it is not going to have any files that are the standard. Instead of these standard files, it is going to have some of the special files that are going to be more representative of the process and the system information that we are working with.
6. /root: This is the root home directory. This is going to be the root user's home directory. Note it is not going to be located in something like /home/root, but instead, it is stored as just /root.

7. /run: This is going to be the application state files. This is going to be a bit newer, and it is going to provide us with a place for applications so that they are able to store their transient files, like the sockets and process IDs. These are not going to be stored in the file for /temp files because this could delete some of the things that we need.
8. /sbin: This one is for System Administration Binaries. This is going to also contain some of the binaries that we need for the help of any system administration by the root user.
9. Selinux: You will find that this is going to be the particular Linux distro that you are able to use for security. The directory is going to contain all of the files that you need in order to work with SELinux. The directory is going to also hold onto all of the files that you need for this, as well. If you would like to work on the Ubuntu system and you see that this directory is there, remember that this is a bug in the program because Ubuntu is not going to use this, just Linux.
10. /srv: This is going to be some of the service data. This is a good place where we are able to find the data for some of the services that are provided by the system. If you were working with the server for Apache HTTP for the website you were creating, you would store all of the files for this website in this directory.
11. /tmp: This one is for the temporary files. This is where all of the temporary application files are going to be stored. When the system is ready to restart or reboot, these files are going to be deleted, and you will no longer be able to find them again.
12. /usr: This is going to contain the user binaries and some of the read-only data. Here you are going to be able to find files and applications that are going to be used by your users, rather than the system. For example, you may find some of the non-essential

applications in this one, along with some of the binaries that are not necessary at this time.

13. /var: This is going to be for the variable data files. When you have the /usr as only readable, the /var is going to be writable. Here you are going to be able to find some of the log files and anything else that the user will be able to write out.

There are also a few different components that you are going to find when it is time to work with the Linux operating system. There are actually three main code bodies that are going to make Linux successful and will ensure that you are able to find some of the different codings that you would like to do with this process, as well. Some of the different components that we are able to see when it comes to working with the Linux system will include:

The kernel is first on the list. This is going to be the one that is in charge of the maintenance of all the abstractions of the Linux operating system, as well as the processes and the virtual memory that we are working with. This is going to be the center point for the operating system that we are working with, kind of like the spine of the system. Because of this, it is going to be the part that is responsible for the functionality that is required in order to run any process, as well as providing the system service that will give us some protected access to the hardware resources. Anything that is required for the operating system to run well will be done and handled by the kernel.

From there, we are able to work with what is known as the system libraries. These are going to be a set of functions that are important because they allow for some interrelation between the kernel and the applications. These are going to apply a lot of the functionality that we need with the operating

system and it will not need to take away the rights or the privileges when it is time to handle the kernel code as well.

And finally, the third part that we need to focus on here is the system utilities. These are going to be the programs that we are able to use in order to execute specific managing tasks or the ones that are a bit more specialized. There are a few utilities that can be invoked just once in order to help initialize the features of our system and then configure them as needed. Others are going to be set up in a manner where they will run constantly, carrying out tasks like responding to the connections of the network, both the ones that come in and the ones that go out, accepting requests for logging on, or even taking the time to update all the necessary files and log records as well.

Chapter 4: The Commands You Need to Know in Linux

The next thing that we need to spend some time on when we work with the Linux system is some of the commands. The Linux system is going to work in a slightly different manner than what you will see when it is time to work with this operating system. Instead of having the graphics that you are able to work with and look through, you are able to work with this operating system with the help of the command prompt. This means that we need to know some of the commands and maybe a bit of coding, in order to get this set up in a manner that we are able to easily use.

That is why we are going to spend some time in this chapter looking at some of the more essential and basic commands in Linux, the ones that you will really need to learn more about in order to fire up this operating system and play along with it as well. As we go through the rest of this guidebook, you will find that knowing some of these commands can help you to get a better understanding of this operating system, and can make it easier to actually work with it when it is time. With this in mind, some of the different commands that we are able to work with when it comes to the Linux system includes:

The Listing Directories and Files

The first thing that we need to take a look at is the command of "ls." When you first get onto this operating system, you will find that you are on the home directory. This is going to come with the same name as you put into

place for the username, and it is going to be where all of the subdirectories and personal files will be saved and easy to find. If you would like to be able to find out what the contents are of your home directory, you would just need to type in the following command to get it done:

% ls.

Now, it is possible that you will do this command; there will not be any files that are found in the directory. If there are none that are present there, then you are going to be returned right back to the prompt. Be aware that, using this command, you are only going to see the contents that are present but that do not have a name that starts with a dot.

In this operating system, if you have a file that starts with a dot, this means that the files are going to be hidden. This also means that there are going to be signs of important configuration information that is found in the file. The reason that they are hidden is that they are set up so that you should not touch them or mess with them.

If you would like to be able to see all of the files, including those with the dot, while still being found in the home directory, you will need to type in the following code to see these:

% ls -a

When we are able to use the coding above, you will find that all of the files, including the ones that are hidden up a bit, are going to be easy to see. Ls is going to be one of the commands that you are able to use for a lot of

different things, and it is good for taking options and the above one is just a few of the options that you are able to work with. When you add on some of these different options, they are really going to change up how this command is able to work with.

Making Some Directories

The next command that we are able to work with is the mkdir option. To make a subdirectory of the home directory, which is able to hold onto the files that you want, you are able to work with the mkdir. We are going to make it simple here and just call it the linuxstuff. But to make this work for our needs, we need to type in the code that is below into the current directory:

% mkdir linuxstuff

If you would like to take it to the next step and see what directory we are working with, we will need to type in the following codes include:

% ls.

Changing Your Location to a New Directory

The next thing that we need to work with here is the command to change ourselves to another directory. We can do this with the cd command. This means that we want the system to change the directory from the current one to another directory of our choice. You can do this over to the directory that we created above. The code that we want to use to make this one happen would include:

% cd linuxstuff.

If you would like to see the content, which shouldn't have anything in it at this point since we have not gone through the process to add anything into that directory yet, we are able to type ls.

The Pathnames

Along with the same idea, we need to be able to spend some time with the command for pathnames, which is going to be pwd. This command is going to stand for the print working directory and it is going to use the pathname in order to let you work out exactly where you are located in the file system. For example, if you would like to know the absolute pathname that goes along with the home directory that you are working with, you would type in cd. This helps you to go back to what is known as the home directory. Once you are in the home directory, you would want to type in the code:

% pwd

When this is done, the results that you should see here is /home/its/ug1/ee51vn. And what this is going to mean here is that the home directory is going to be found as the subdirectory known as ug1. This is going to be located in the subdirectory that we called "its" which is going to also be located in the subdirectory of home, in the top level of the root directory that we are going to have named /.

This may seem like a lot of information to handle right now, but this is showing us that there are a few levels of things that we are able to work with at this time. You went from one level to the next, and down even further until you found the subdirectory that we wanted to handle right now. You will be able to take a look at the pathname in order to figure out how

many times or subdirectories we need to go down in order to make this process work.

We need to spend a bit more time here looking at some of the pathnames and what we are able to do with them. If you are not currently in the home directory that is on our system, we need to get ourselves back there. We are able to type in the code below to help us get back over there:

```
% ls linuxstuff
```

This is going to spend some time listing out the contents that are found in the home directory. When we are found in this part of the code, we will want to type in the following code to help us get started:

```
% ls backups
```

At this point, you are going to get a message to show up, and it is going to say something like “backups: No such file or directory.” Why does this happen? It is because you went through the process and created a directory with that name earlier on, but you didn’t create it in the working directory. So, to get to the backups directory that we have, you either need to use the cd and then specify the directory that you have or you need to work with the pathname. A good code that we are able to use to make this happen will include the following:

```
% ls linuxstuff/backups
```

This is going to be the name of our home directory. We are also able to work with what is known as the tilde character (~)to help us refer ourselves back to the home directory and to make sure that we are able to specify a path that is going to start out with the home directory. So, if we stopped and typed out code like the following:

```
% ls ~ /linuxstuff
```

You would end up seeing a list of what is all in the linuxstuff directory. This is going to happen no matter where your current location is in that file system. This can ensure that you are able to see what you would like in the system, without having to click on a bunch of things or getting yourself lost.

Copying the Files

Another thing that we are able to work with is copying the files so that we can put them somewhere else or have them set up in the manner that we would like. The command that we need to work with here is “cp.” If you would like to copy file1 that is found in the working directory, and then name it file2 instead, you would need to work with the following code to make it happen:

```
cp file1 file2
```

Removing a File or a Directory

The next thing that we need to consider working with is removing a file or a directory when we no longer what to work with this one at all. We would work with rm to help remove the file and we can then work with rmdir in order to remove the directory that we would like to use.

To get a better idea of how this is going to work, we are going to take a few steps and see how it can happen for us. Let's make a copy of the science.txt and then go through and delete it as well. To do this, we need to go to the linuxstuff directory that we did before and type in the code below:

```
% cp science.txt tempfile.tx
% ls
% rm tempfile.txt
% ls
```

If you want to go through this process and get rid of an entire directory along the way, we first need to go and check whether there are files in it or not. We need to have it free of all files and then we can work with the rmdir command. You can have a go at going onto your system and removing the directory that is there that is known as Backups. You will find that as it is right now, this is something that Linux is not going to allow because there is an item that is found in it. Once you remove that item, then the command will work.

How to Display File Contents on the Screen

The next thing that we are able to work with is how to display the contents in the file on the screen. This is going to need the help of the clear command to help it work. Before we move on with the rest of the things that we are able to do, we are going to spend a few minutes clearing out the terminal window of all the commands that are already typed in so that we can better understand the output of the next command as well. The code that we need to use to make this happen includes:

% clear

When you use this command, all of the text is going to be removed so that you end up with just a prompt left. This means that we need to move on to the next command. And this command is going to be “cat.” This command is going to be used in order to concatenate and then display the content of the file on your screen. A good example of the code that we are able to use to make this happen is going to include:

% cat science.txt

You will find that when you dot this one, the file that you end up with is going to be bigger than the size of the window. This means that you will need to scroll through it to figure out what is all there and that makes some of the contents a bit harder to read through as well. This is where we are going to work with less command. This command is going to help us to write the contents of the file on the screen, doing it one page at a time. The code that you are able to use in order to make this happen to include:

% less science.txt

When you have this, all of the information is going to show up on its own page. You can press on the space bar if you would like to see the next page and do it a few times if there are more than two pages that you would like to work with. When you have had a chance to read through the information, and you do not need it any longer, then just type in q.

One thing to note here is that if you have some files that are long, you may want to work with something else. Working with the command of less rather than the cat command is going to be better when the files are really long because it can prevent some of the issues of taking up a lot of space.

Another command that we need to look at that falls into this category is going to be “head.” This is the command that you are going to use when you just want the first ten lines of the file that you specify to show up on the screen. This can give you a kind of preview to see what is going on with the file and helps you to see if it is the right one for you. If you would like to work with this particular command, make sure to clear off the screen and then type in the following command:

```
% head science.txt
```

Rom there, you are able to type out the following:

```
% head -5 science.txt
```

Type that one in and see if it makes a difference in the output that you are going to get from this whole system. Then we are going to work with the tail rather than the head here. In contrast to what we are going to see when we work with the header command, this tail command is going to write out the final ten lines of the file that you specify on the screen. To work with this one, we will just want to work with the following code:

```
% tail science.txt
```

This one is a great option to help you see whether the file is complete or not. You get a chance to look at the final bit of the file that you have and you can read through it to see what is there, whether it is complete, and more.

How to Look Through the Contents of a File

Now it is time for us to take a look through some of the contents that are found in one of the files that we are working with. You will find that the less command is going to help with this one. Using this command, you are able to search for a pattern of keywords in a text file. For example, if you wanted to find all of the instances of the word science in this kind of file, you will be able to type in the code below:

```
% less science.txt
```

And then, staying with the less command, if you work to type in the forward slash, along with the word that you would like to search for, you can get the search all done. A good example of doing this is going to be below:

```
/science
```

All of the instances of the word that show up in that file are going to be highlighted. If you would like to find the next instance, though, and go through the file to see where all of these instances are, you would type in "grep." This is going to be one of the standard utilities that are found on Linux and it is going to be used to help us search for some of the specific words or patterns that we need in the work that we are doing. To make this

one work, we need to clear off the screen and then type in the following command:

% grep science science.txt

Now, you should be able to see that the command of grep is going to print on all of the lines that have the word science in it. But is that the end of it? At this point, we are going to type in the code below:

% grep Science science.txt

What this shows us is that the original one did not find all of the instances. And this is because the grep search is going to be case sensitive. It is going to see that there is a difference between Science and science. If you would like to ignore the case sensitivity and make sure that all of the instances of science show up, whether they are in uppercase or lower case, you would want to add in the -i. For example, you would type in the following code to make this work:

% grep -I science science.txt

If you would like to search out a specific pattern or a phrase, this is possible, but you need to make sure that you are putting that all inside of some single quote marks in order to get it to work well. To search for a spinning top, you would type in the following code:

% gep -I ‘spinning top’ science.txt

There are a lot of other options that we are able to use to make this work for our needs, as well. Some of the other options that come with the grep command will include:

-v: This one is going to display for us the lines that are not going to match the specified text.
-n: This one is going to precede each of the matching lines with the correct line number that we are working with.
-c: This one is only going to print out the total number of matching lines that we want to work with.

Appending Files

The next thing that we are able to work with is how to append our files. We are able to work with the (>>) symbol in order to append the standard output to a file. So if we are working with this and would like to add in a few more items to our list1, we would be able to type in the code below to make this one happen:

```
% cat >> list1
```

When this is done, you would need to type in the names of the other fruits that you would like in the order that they need to be in when you do the file. Then, when the list is complete, you will click on CTRL + d to stop. To read the contents of the file, you can type in the code below:

```
% cat list1
```

You should now have two files. There is going to be one that will hold onto the six fruits that you are working with and then there is another list that is

going to have four fruits. We will want to go through and combine together the two lists so that they are able to do the work that we want in no time. The cat command is going to help us to get all of this done and the coding that we are able to use to see this one work well will include:

% cat list1 list2 > biglist

This one is going to work out well because it is able to read the contents of both lists, in turn, and then will output the text from each so that it goes into a new file. Thanks to how we set this up, it is going to call the new file that we just created biglist. If you would like to be able to read through the contents that show up with the biglist, we need to type in the following command:

% cat biglist.

The Help Command

Another thing that we are able to spend some time here is the help command. There are a lot of manuals that you are able to find online that are going to provide you with some of the information that you need on these commands. The pages of these manuals can come with a lot of the information that you need when it comes to what the command is able to do, the options that it will take and how all of these options are going to be able to make some modifications to the command.

If you would like to read the page for one of the specific commands that we have, you would want to type in “man.” For example, let’s say that we want to go through and know a bit more about the command of wc. To do this, we could type in one of two codes including the two below:

% man wc

% whatis wc

This one is going to be useful because it is going to provide us with a small and quick description of the command. Keep in mind with this one, though, that it is not going to provide us with more information. You will not have any information about the options or anything else that goes with it. You would have to do some other topics in order to get things started and to gather up some more information as well.

As you can see, there are a lot of different things that we are going to be able to work with when it is time to bring out some of the commands that we will use in this language overall. You will find that handling all of these commands will work well when it is time to bring up different parts of the operating system, some of the files that you would like to work with and so much more. Make sure to take a look at some of the different commands that come with this, and see just how great this can be for your needs.

Chapter 5: Teach Yourself to Fish

The next option that we are able to work with is the idea of teaching yourself to fish. This may seem a bit silly right now, but as we go through this chapter, you will find that it makes sense and can really help us to do more when it comes to working with our Linux system. Keep in mind that all of the codes that we are going to work with will include https://fishshell.com

Fish is going to be a command-line shell that is similar to Bash, which is going to be really easy for the user to work with. You will find that it is able to handle a lot of the most powerful features, including things like tab completion, highlighting the syntax and autosuggestions. You will not need to worry about a ton of configurations along the way, and there is not a lot that you have to learn to do this work.

If you are trying to find a productive command line, one that is a lot of fun and more useful than some of the others that you may have used in the past, then fish is probably the method that will work the best for your needs. And we are going to spend some time looking at how to work with this command line and a lot of the neat things that we are able to concentrate on when it comes to this command line:

Learning Fish

The first thing that we need to work with here is how to work with the Fish command shell. We are going to make the assumption that you have gone through and worked with some of the shells and commands that are found with the Linux system, so you are ready to go. And now it is time to work more with Fish and how we are able to make this work.

To do this, we have to start out by downloading the fish shell and then we can get started. When it is downloaded, you can open up the Fish command line and then see a message that says something like "Welcome to fish, the friendly interactive shell." You are tenable to type for help in order to get some of the instructions that are needed on how to work with the fish program. The code that we need to make this one work will include:

you@hostname ~ >

Fish is already going to come with a default prompt in that it is going to show off all of your details when you do this. This means that things like your hostname, username and the current working directory that you would like to work with are going to show up when you do this. We will take a look at how we are able to make some changes to the prompt later on, but we are going to take a look at it this way for now.

Running Some Commands in Fish

We need to spend some time learning how to run commands in this command shell. Running some of the commands that you would like in fish is going to be the same as you are able to do with some of the other shells that are there. You will just need to type in the command, along with some of the other arguments that you need to go with it. The spaces are going to

be the way that we are able to separate this out. This is going to be similar to some of the commands that we talked about earlier in this guidebook as well. Let's look at an example of this one below:

```
echo hello world
```

And when we do this, we are going to get the output of hello world to help us out.

There are a lot of commands that we are able to work in order to really help us to get started with this option, and we are going to spend some time looking at how to make this work for our needs. To start, we are going to work with the Help command. Fish is going to include some of the best manuals and help pages that we are able to work with any time that we are questioning what we are doing or trying to figure out which steps to take next as well.

To get started, we simply need to run the help command, and it is going to open it up in a new web browser. Or you have the option of running man, and then the help file will open up for you in the man page. You are also able to find some help on the specific commands that you are confused about. So, if you would like to have a man set to see help in the terminal, you would want to work with the following code:

```
> man set
Set – handle shell variables
Synopsis…
```

Another thing that we are able to work with when it is time to handle some of the commands in this shell is the idea of syntax highlighting. You may notice that just by spending a short amount of time working in Fish that it is going to be able to highlight the syntax that we are on when it is being typed out. If you see that you are working through this and you notice that it is being highlighted in red, then this is a good sign that the command is not valid.

This may be because the command is either one that does not exist or because you are writing out codes that re-referencing a file that we are not able to execute. When the command is actually valid, or you make the necessary changes to turn it into a valid code, then it is going to change colors.

Another thing that we need to work with is that some of the paths that are valid files are going to be underlined when we type them out. This is going to let us know that there is a file that is on our system that has that name. This can be useful when you are typing out the codes because it ensures that you are able to find what you would like.

We can also work with the wildcard as well because it is something that Fish is able to support. If you would like to look at all of the JPEG files that we have, you would type in something like the following:

```
>  ls * .jpg
Leno.jpg
Moona.jpg
Sana margarita.jpg
```

It is even possible to go through and work with more than one wildcard based on what is going to work the best for some of the work that we are doing. From there, we are able to finish up with some pipes and redirections if those work out well with our code. This means that the Fish shell is going to support the use of the vertical bar, which is for our pipe command and you can use it for piping between the commands.

Autosuggestions are another thing that we are able to focus on here, as well. As you spend some time typing out the codes that you want to use in Fish, it is automatically going to get to work, suggesting commands. You will see that these suggestions are going to be shown to the right of the cursor and will be highlighted a bit in gray. You can choose whether you would like to work with these or not.

The Fish shell is also going to know a bit about the history of what you have done with coding in the past, which is going to be important and can save us some time and hassle as well. We are able to type in the command that we want to use. And then, when it is time to use it again, we can then start to type it all out again so that the full command is going to appear without having to worry about it the whole time or typing the whole thing out.

If you would like to accept the suggestion that it is given, you can press the right arrow key to let it come into the shell. If you just want one word of the suggestion, this is possible as well. If you just want to work with the one word, then you would hit the Alt + right arrow key. If the suggestion is, of

course, and it is not what you want, you can ignore the suggestion and then move on to the next step to make this one work for your needs.

If you would like to be able to accept the autosuggestion, you can hit the CTRL + F to accept just the single word; you can work with Alt and right arrow. And then, remember to just ignore it if you do not want to work that particular autosuggestion at all.

Another thing that we are able to work with is tab completions. There are going to be a lot of tab completions in fish that work without any configuration whatsoever. To make this happen, we simply need to start by typing in an argument, path, or command, and then we are able to press on our tab key to get this to be complete. It is also possible to work with two or sometimes more suggestions. And this is a possibility; then we need to list them out in that manner as well.

The Variables

When it is time to work with any kind of coding language or shell, we need to work with the variables. As with other shells, the dollar sign is going to be used to perform some of the variable substitutions. It is also possible to do this with some double quotes if you would like, but never substitute these with single quotes, or it is not going to work the way that you would like.

However, we have to remember that there is not necessarily going to be some syntax that can be dedicated to setting this kind of variable. Instead, the Fish shell is going to use an ordinary command that we are able to call "set." This is going to take the name of the variable and then the value of the variable and use these in the manner that we need.

We always have to worry about the quotes. If they are not used, then you can put in one phrase with two words and they are going to be seen as two separate arguments, then we would have to worry about two lists of elements as well. In addition, when we work with Fish, the variables are not going to be split after we have provided them with a new substitution.

On the other hand, if you are in the Bash shell, you would end up with two directories when you are doing this. But in the Fish shell, we can get one and then we would pass any of the arguments that we are working with over to the mkdir.

The Lists

Another thing that we need to take some time looking at is the list. We have to remember before we get into this one that all of the variables that we work with are going to be classified as lists and they are going to contain no values or any number of values.

It is also possible that the variables we work with are going to come with just one value. And one of these is going to be the $PWD. Conventionally, we would talk about the value of that variable, but when we look at it in reality, it is the only value it has. Other variables have several values, like $PATH. During the expansion of the variable, you will be able to extend it out to more than one argument if you would like.

A list is not going to be able to contain any other list; there is no such thing as recursion here. A variable is going to contain a list of strings and that is all that you will find inside. If you would like to figure out what the length of the list is, you would need to use the count command.

You can append and add some more to the list by setting that list to itself and then adding in the extra arguments that are needed. In this example, we are going to append /usr/local/bin to the $PATH. The example of how we would work with this one includes:

```
>  set PATH $PATH /usr/locale/bn
```

We will want to make sure that we are working with the square brackets to help us access all of the individual elements that are needed. Indexing is going, to begin with, 1 at the start, and then we want to work from the end, we would start with the -1 to make this all work. An example of how this is going to work will be seen below:

```
> echo $PATH
/usr/bn /bin /user/sbin /sbin /usr/localn/bin
> echo $PATH [1]
/usr/bin
> echo $PATH[-1]
/usr/local/bin
```

Fish also allows us to take this a bit further if we would like and we are able to access some of the slices in our code. This is going to basically be the range of elements. We are able to work with the options that are above but add in the different numbers that we are able to work with, or the range, rather than just one number.

And, similar to what we are going to see with any other kind of computer that we are working with, or even with other programming languages, we will be able to work with the “for loops” to make it easier to iterate over the list that we would like.

The Command Substitutions

The next thing that we need to take a look at here is the command substitutions. Command substitution is going to be when the output of a command is going to be used as an argument to a different command. Unlike some of the other shells that you may have spent some time working with in the past, there is not going to be anything like a backtick in Fish for this. Instead, we are going to work with the parentheses to show this off.

One of the most common of the idioms that are present in this shell is to use a variable in order to capture some more of the output from the command. But the command substitution that we are doing is not something that we want to expand out inside of some quotation marks. Instead, the quotes have to be closed for a bit and then we can add in the substitutions of the command when these are closed. When it is all done, we are able to re-open the quotes and all of this can be done in one argument.

While we are on the topic, there will be something known as combiners that we are able to handle in a lot of the different shells out there. However, there is not going to be one special syntax in the Fish shell that is going to help us to combine together the commands. Rather, we are able to work with three commands to make this work including or, and, and not.

Functions

Another thing that is important for us to work with when it is time to handle any of the codings that we want to do in the Fish shell is the idea of the

function. When we are in the Fish shell, the functions are going to be the lists of commands, which sometimes will count as arguments and other times will not be. We are not going to pass the arguments as numbered variables here. Instead, we are going to pass them as single lists instead.

There are going to be a lot of different types of functions that we are able to work in order to help us out. The first type will be a built-in function. And in the Fish shell, they are going to be able to help us create some of the functions that we would like to work with.

In addition, we have to remember that there is not going to be a prompt or any kind of special syntax that is needed here and there will not be any aliases that show up. Functions are going to have their own unique place in his code, and you are able to use the functions keywords to make it easier to list out all of the names of the functions. Keep in mind that the Fish shell is going to come in with a large number of functions that we are able to work with. Unlike the other shells, though, Fish is not going to have a special prompting syntax or aliases that we use in the code because the function is going to take the place of all of these.

$PATH

The next thing that we need to spend some of our time on is the $PATH option. This is going to be one out of several environment variables that we are able to use here, and it is going to be the home of all of the directories that we will use for commands in the Fish shell. $PATH is not going to be delimited as a string, but it is more of a list. If you would like to prepend some of your paths to work with this, you would write out the code:

```
> set PATH /usr/local/bin /usr/sbin $PATH
```

You are able to do this with the help of config_fish, or you do get the option to modify the universal variable if you would like to make sure that you can automatically prepend the $PATH ahead of time. The major benefit of working with it in this second manner is that there isn't going to be the need to mess around with any of the files. All that you will need to do to make this one work is run the command once in the command line and then the changes will happen in both the current session that you are doing and in some of the ones that happen in the future as well.

One thing to keep in mind here, though, is that you do not add the code line over to the config_fish. If you do this, then the variable is just going to cause a mess because it grows in size each time that you do use this program, whether it is done in the right manner or not.

As we can see, there are a lot of different parts that we are able to work with when it is time to handle some of the parts of the Fish shell. This one is going to allow us to work with a lot of the same commands that we talked about before, which is going to make it so useful for a lot of the different needs that we have. With this in mind, let's take a look at a few of the other things that we are able to do with the Linux system and how we are able to expand this out for some of our own needs as well.

Chapter 6: How to Handle Your Editors

There are going to be a lot of text editors that we are able to work with when we handle some of the things that we want in Linux, so it is easy to become a bit confused when we need to put all of this together. We are going to narrow it down a bit to make life a little easier for someone who is just getting started with the Linux operating system for the first time. And this means that we are going to spend some time looking at the *nano* and the *vi* editors, which are two of the basic text editors that we need with Linux and will still provide us with some of the power that we are looking for.

Nano

Nano is going to be something that we find installed on a lot of the distributions of Linux already, and it is going to work well when we bring out Sudo. This is why we need to spend some time talking about it and seeing how we are able to work with this for our needs.

First, we need to take a look at how to run Nano. There are two main ways that we are able to run this text editor to get it up and working the way that we want. The first one is that when the command prompt gets started, we just need to type in "nano." The second one is that we are able to input the command of "nano/name of file" and that will do it. You can insert the name of the file and then nano will take the time to look for it. If this file is

found, then Nano is going to open it up. If your editor is not able to find it, then you will get the empty bugger that has the same name as the filename.

At this point, we can look at the top of the screen, and we are going to see some information there about the file that we are working with. If we are not currently in a file for this one, then it is going to say, New Buffer. Following that is going to be all of the content of your document in the form of text. Then there will be some information in the system that will provide us with the necessary data on how to get things started.

The first thing that we are going to work with on this one is some of the shortcuts that we are able to focus on. These shortcuts are going to be program functions like saving and exiting, and we are going to be able to look near the bottom of the screen to see some of these when we are in Nano. You will not need to use SHIFT when you want to work on the shortcuts, and they are going to be in lowercase and an unmodified number format.

To start here, we will look at how to save a file. Doing this is going to be known as “writing out,” and you are able to do this with the CTRL + O. Next, you will be asked for the name and the shortcuts that will change to show you what we are able to input to finish the command.

If we would like to be able to insert the contents that are needed from another file into the one that we are working with, we can type in CTRL + R and help us cancel both of these commands, then we just need to press on CTRL + C. If you have any trouble with this key, then you can just press on ESC two time. And if you see some commands that are going to ask you to

work with what is known as the Meta key, then the Alt key is going to be fine. And we are able to work with the CTRL + X to help us exit out of what we are doing at the time.

There are a few other methods that we are able to use in order to navigate one of the text files that we want to handle. In order to navigate this kind of file, you are able to use a few keys, including the array key, page down and page up, end keys and home. If you would like to use those, you will be all set, but there are a few other shortcut keys that we are able to use to make ourselves more efficient at the work that we are doing in our editor. Some of the other keys that we need to know how to work with if we choose include:

1. CTRL + F: This one is going to move the cursor forward.
2. CTRL + B: This one is going to move our cursor to go backward.
3. CTRL + P: This one is going to move the cursor to go up by one line.
4. CTRL + N: This one is going to move the cursor so that it goes down by one line.
5. CTRL + A: This one is going to take the place of the Home key that you would like.
6. CTRL + E: This one is going to take the place of the End key that you may have used in other options.
7. CTRL + V: This one is going to help us to move down just one page.
8. CTRL + Y: This one is going to help us to move up one page.
9. CTRL + SPACE: This one is going to make it easier for us to move forward just one word at a time.
10. ALT + SPACE: This one is going to make it easier for us to move backward one word at a time.

11. CTRL + C: This one is going to indicate where the cursor is located at any given time when you need it.

Working with Vi

Now that we have had some time to look over how to work with the Nano version of this, it is time to look at the command line editor that is known as Vi. This is going to be a really powerful command-line editor that you are able to choose, but it is going to be plain, similar to the Notepad that we are able to find on Windows. And to use it, we have to rely simply on the keyboard, rather than the mouse. For some people who are just getting started with all of this, that may seem a bit awkward, but it ensures that you are going to get the most out of this.

Vi is going to come with two main operating modes that we are able to focus on. These are going to include the Insert of the Input mode and the Edit mode. In the Insert mode, you are able to insert content into the working file that is current and then when we are in the Edit mode, you are going to spend your time navigating around the file, performing things like copy, delete, search, replace, save and more.

Setting up the Vi command-line editor and making sure that it is running the way that you would like is going to be pretty simple. You just need to type in one command-line argument that is going to contain the file name that you are hoping to edit with this. An example of how we would get the Vi editor up and running includes:

Vi <name of file>

If you want to get started with this without having to specify a filename, you are able to go through and open it up from within. Just keep in mind that it is much easier to must close Vi down and start it up again. But the choice on how to handle this is up to you.

Like with the other option, we need to take a moment to look at some of the steps that we should take in order to navigate with this command-line editor. These commands are going to be a bit different compared to what we are used to with some of the others, and it is even a bit different compared to what we did with Nano before.

For this one, we want to make sure that we are able to open up a file to work with again and then get ourselves into the insert mode. You will need to enter in a few paragraphs here, the content does not really matter we just need to have something there and then click Esc so that you are able to get yourself back into the editing mode from before.

To help you go through and navigate around the file that you are using, you will need to work with some of the following commands. Do some of these in real-time so that you are able to see how they work and get a real-life look at the things that they will use when it is time to handle your document or your file:

1. You can first work with the arrow keys. These will help you to just move the cursor around as needed.
2. J: This one is going to move the cursor to go down.
3. K: This one is going to move the cursor to go up.
4. H: This one is going to move the cursor to the right.

5. L: This one is going to move the cursor to go to the left.
6. $: This one is going to move the cursor so that it ends up at the end of whichever line you are on right now.
7. ^: This one is going to help us to end up back at the start of the line that we are on.
8. nG: This one is going to move us over to what is known as the nth line. For example, if you are writing out 6G, it is going to take you to the 6th line in the file.
9. G: This is going to move us over to the final line that is in the text that we want to work with.
10. W: This one is going to move us to the start of the next word, based on where we are right then.
11. Nw: This one is going to help us to move forward a certain number of words. For example, if we are working with 4c, then this means that we want the program to move us forward by four words.
12. B: This one is going to ask that the program takes us to the start of the last word.
13. Nb: This is going to take us back to the word that we specify out in the code.
14. {: This one is going to ask the command-line editor to take us back by a paragraph.
15. }: This one is going to ask the command-line editor to take us forward by a paragraph.

As we can see here, both of these text editors are going to be useful for what we would like to do in some of our codings. But often, it depends on what we are hoping to get out of the process and what results we think we can get from both. There are also some other command-line editors that you

are able to work with, so before you decide on the right one, do some research, see which features are available for each one and then work from there to choose the best one for your needs.

Chapter 7: The Necessary Permissions

Another thing that we need to consider when we are working with all of these is the permissions we want to give out. This can include both the files and the directory. You most likely, for security reasons, do not want to provide full access to the files and directories to each person who is going to come by, and this is why we need to go through and come up with some of the best file and directory permissions right from the beginning.

That is why this chapter is going to spend some time looking at the steps that are needed to set up these permissions. These permissions are important because they are going to be used in order to specify what the user can and can't do with a particular file or a directory. This is going to help us make sure that any of the working environments that we have are as secure as possible. You don't want to allow someone to mess around with the files and then causing some issues, so we will work with the Linux system to add in permissions and keep it all safe.

Permissions are going to dictate what you and others are able to write, read and execute when it comes to the directories and the files. We are able to look at these and see that there is a single letter that goes with each one. So, *r* is going to be the permission to read, which allows the users to read the contents of a file. Then there is *w* for write, which allows the user to go

through and edit some of the contents that are in a file. And *x* is going to be the process of executing, which is going to allow the user the permission to run files as if there were a program or a script.

For each of the files that we are working with, we will notice that there are three users that we can define. Knowing these can give us a better idea of the different options that are there and the permissions that each one is going to work with. For example, there is the owner, who is the person who is the owner of the file. Often this is the person who was responsible for creating the file in the first place, but this is not always the cause. Then there is the group, which you will find that each file is going to belong to one of its own groups. And then there are others, which is going to catch anyone who isn't going to fall into the two sets that we had above.

So, we are going to find that there are three main types of permissions that we are able to work with, and then there are three users. And these things are going to be the summary of these permissions and how we are able to work with them. But with this in mind, we need to go through and take a look at the steps that are needed in order to edit them.

Viewing Permissions

If you would like a chance to view the permissions that are on a file, you will need to work with the ls command and make sure that it is going to have a long-lasting option that comes with it. We can take a look at how this code is going to look below:

Ls = l [path]\
Ls – l /home/ryan/linuxtutorialwork/frog.png
-rwxr – x 1 harry users 2.7K Jan 4
07:32/home/ryan/linuxtutorialwork/frog.png

When we take a look at this example, we need to take a look at some of the first ten characters that are going to help us see the permissions that are allowed as an output. For example, the first character is going to tell you what the type of file is. If it is a *d*, then that is the directory and it is an ordinary file that we can work with here.

Then we can look at the next three characters to see what the permissions of that file are for the file owner. A letter tells you that there is going to be some permissions in place and then will identify which one. We will see that the (--) is going to tell us that there are not permissions here. In the example that we worked with above, the owner of this file has the permissions to go through and do anything that they would like to this file, including reading, writing and executing the file.

The next three are going to tell us which permissions the whole group is going to have. For this example, the whole group is able to read through the file if they would like, but they are not able to write on it or execute it. You should note here that the permissions are always going to end up in the same order with reading, write and execute.

And finally, we are at the last three characters. These are going to be where we will find the permissions for everyone else, or for the others. For this

one, the only permissions for the others are to execute the file, rather than being able to write it or read through it.

Changing the Permissions

If you have done some of the steps above, but then you find that you would like to change up the permissions of the file or the directory, then you need to work with the command of chmod. This is going to stand for change file mode bits, something that is a bit long, but all that you need to remember is that the mode bits because these are going to be the indicators that we need for the permissions. A good code that we can look at for this one includes:

Chmod [permissions] [path]

The permissions arguments that we are able to work with on this command have been set out in three main components that we are able to work with. For example, the first one is who the permission is being changed for. This could be the users, the owner, the group, others, and all depending on what you are trying to do here. Then we are letting it know whether we are granting or taking away the permission we will see the + or – sign in order to see this. And then finally we are going to put in information about which permissions are being set here. Remember that we are able to work with reading, write or execute so stick with those.

Shorthand to Set the Permissions

While the methods that we have been talking about above are going to be easy to use and will make it possible to work on some of the permissions that we would like, it is going to end up being a bit long if we need to go through and set up some specific permissions for specific files on a regular basis. The good news here is that we are able to work with a somewhat shorter version of this if we would like.

To understand this method, though, and how it is meant to work for us, we need to really get into the number system in Linux. The normal number system is going to be all about the decimals, with a base 10 number. And it usually goes from 0 to 9. We also have the octal number system, which is going to be a base 8 system and goes from 0 to 7. There are also three permissions that come up with this one, and each is either going to be on, or it is off, and as such, there will be 8 combinations that we are able to work with.

It is also possible for us to go through and work with binary in order to represent these numbers. When it is time to handle binary, we get two options, the 0 and the 1. The following will show us how some of the octal numbers are going to be mapped out when we work with the binary numbers:

0000
1001
2010
3011
4100
5101
6110
7111

What your mind find a little bit interesting here is that we can just use three of the binary values in order to represent the 8 octal numbers each time that we work with each possible combination of the 0 and 1 in our work. So,

there are going to be three bits and there are also three permissions that are allowed. You can use 1 to represent on in this, and then 0 can represent off, and that means that one octal number can be used in order to represent permission set for the users that you choose. If we work with all three of the numbers, then we can represent the permissions of all three, including the owner or users, the group and others while we are there.

Basic Security to Follow

While we are on the topic here, we need to spend a little bit of time looking at the basic security that is needed in our Linux directories. Your space on the Linux system is going to be the home directory and it is going to be your responsibility in order to make it stay safe and secure all of the time. Some users are going to choose to give themselves the full permission that is necessary to read, write and execute, but will not provide any permissions for others or for the groups. And some will allow for a few permissions to the others and the groups. Each owner will need to set it up to work the best for their needs.

To get the best security on the directory you are using, you should not give the group, or any of the others, the right to access your own home directory. But you can provide them with some execute permissions so that they can still use it as needed, without adding on the read permissions. If you choose to do this, other users are going to be able to access your home directory, but they will not be able to see what is there. A good example of this one is going to be your own personal web pages.

Some systems are responsible for running web servers and give each of their users a webspace all to their own. The most common of these is to

create a directory that is found in the home directory and call it public_html. This allows the server to read it and then to display what is found inside of it as well. However, because we will find that the web server we are working with is not going to be the same user that you are, it is not able to get in and it won't be able to read the files. In this kind of situation, it is going to be necessary for permission to execute to be given on the home directory before that happens.

If you provide this permission, it is going to allow the webserver user to get to the resources that they need. But all of this is going to be up to you and what you would like to see done with the whole system as well. Sometimes the information is not that sensitive or you don't mind if a few of the groups or other people are able to get some access to change it. And sometimes the information needs to be left secure so that only you are able to make the changes as well. It is all going to depend on what your directories are about and how secure you need to keep that information as well.

As you can imagine here, there are a lot of parts that come with providing permissions when you work with the directory that you are in. Being careful with the permissions that you are allowing is going to make a big difference in how successful this process is going to be, and will ensure that we are able to really keep our information safe and secure overall as well.

Chapter 8: Looking at the Variables of Your Environment

The environment variables are going to be some of the objects that are given names and will be able to contain the data that will be used by a minimum of one application, though there is usually more than one application that is relying on it. To keep it simple, the environment variable is just going to be a variable that has both a name and a value that is attached to it.

This means that the environment variable values could be the default that the editor has given to it, or it could be something else as well. Newbies who have not had much time working with Linux may find that it can turn into something that is a bit cumbersome, but the environment variable is still a good way for us to share the settings of configuration between more than one application and process in the meantime.

Utilities

The first thing that we are going to take a look at here is known as the utilities. The package that is known as coreutils is going to be home to the *env* and the *printenv* programs that we are going to need at this point. If you would like to be able to go through and list out all of the current environment variables that we can access, and that also has some value right now, we would need to type in the following code:

$ printenv.

Some of the variables that we are going to work with are kind of user-specific. And there may be times when we will want to check on these and see if they are the right option for us, or at least check that they are still providing us with the information that they need. We can do this when we compare the output that we get as the normal user and then checking it again when we are the root user. If they are the same, then we can see that they are not user-specific in the first place.

In addition, the utility that we are going to call *env* is going to be used to help us run some of the commands that we would like in the environment that was modified for some reason or another. The code that we are going to have below is going to help us run the *xterm* with the help of the EDITOR, the environment variable, and it is going to be set to *vin*. This is going to have absolutely no effect on the global version that we are able to get of this same variable. The code that we are talking about here will include:

$ env EDITOR = vim xterm.

How to Define the Variable

There are going to be a few methods that we are able to use when it is time to handle our variables. First on the list is the global variables. Most of the distributions that you are able to use of Linux is going to ask you to change or add the variable definitions in the path of/etc/profile, or to some other location that makes the most sense to what you are trying to do.

However, before you just do this without thinking, we have to remember that there are going to be a few of our configuration files that have to stick with certain packages or they will not work well. And when this is necessary, these environment variables may have some settings that they need to focus on and remain with as well.

These variables, in particular, have to be managed and maintained, and you need to pay some special attention to all of the files that could be found with that environment variable as well. With just the principle here, any of the scripts that utilize a shell are able to initialize an environment variable. But if we are working with some conventions that are a bit more traditional, then we have to remember that these statements should not be found in all of the files, but only in a few of them.

More to Learn Here

Now that we have had some time to look at a few of the different parts that we are able to work with there here, there are a few terms and topics that we need to know as well, before we can really get through some of the work that we would like to accomplish on the Linux system. Some of the other topics that we need to follow through with include:

1. DESKTOP_SESSION: This is going to be similar to the DE that we talked about before, but it is going to be used inside of the environment of LXDE as well.
2. PATH: This is going to be the home to a list of directories that we have and they are all going to be separated by colons. And this is where our system is going to head through to look for any files that we are able to execute. When the shell is able to go through a

command that is seen as regular, such as the ls that we talked about before, it will start to take a look at any executable file that has the same name as the command that is in the listed directories, and then it is going to execute it as well. If you are doing this process and you would like to run some of the executables that have not been put into this PATH, you need to use the path that is absolute and then pick out a specific executable to make it work.

3. HOME: This is where we are able to find the exact path that is going to lead over to the home directory where the user is logged in a. This can be used by more than one application in order to associate some of the configuration files with the user that is already running that particular variable.
4. PWD: This is where we will be able to find the right path in order to lead to the working directory, as well.
5. OLDPWD: This is where you will find the path that is able to lead to the previous working directory. This means that the value of the PWD had before the last execution of cd.
6. SHELL: This is where we are going to be able to find the right path that can lead us over to the shell that the user prefers to work with. This may not be the shell that they are currently using, depending on some of the preferences that you have as well. No matter which method, the variable is going to be set with the Bash shell when you get it started up.
7. TERM: This is going to contain the type of terminal that you are running at this time. This is going to be used the most often by the program that is going to run in the terminal and the need capabilities that are going to be specific to the terminal that you handle.

8. PAGER: This is going to be one of the commands that will run the program, which is in use to list the contents of the file if you would like.
9. EDITOR: This is going to be the command that we are able to use for running the light programs of file editor. For example, you could write a switch that is more interactive between nono or gedit under X.
10. VISUAL: This is where we are able to find out the command that will run the full editor and it is used for some of the more demanding tasks like mail editing.
11. MAIL: This is the place where we are going to be able to find the location of any incoming mail. The setting that we will often use for this one is going to be /var/spool/mail/$LOGNAME
12. BROWSER: This is where we are going to find the path that will lead us right to our web browser. It is useful to work with when we would like to come out with an interactive configuration file that is set for the shell because it can be altered in a more dynamic manner, depending on how available our graphic environment is in the first place.
13. MANPATH: This is the place where we are going to be able to find out a whole list of directories and we are going to separate them out with some colons. This is also where the man will search for man pages.
14. INFODIR: This is going to be the list of directories, which is also separated out with a colon and this is where the command is going to spend some time looking for info pages when needed.
15. TZ: This one is going to be used when it is time to set some of the time zones, especially when you need it to be different from the one that is on the system. If you take a look inside of the

usr/share/zoneinfo, you will be able to see the zones that we are able to see as our references.

As we can see, there are a lot of different things that we are able to do when it comes to working in the Linux system and getting it all set up for some of our own needs. Even a little bit of this can ensure that we are able to use this in the right manner and that we will be able to get the whole system set up in the manner that we would like in no time.

Chapter 9: Linux and Hacking

The last thing that we are going to spend some time on is looking at how we can work with the Linux system to help us complete some of the ethical hacking that we would like to do. While we are able to do some hacking with the help of Windows and Mac, often, the best operating system to help us out with all of this is going to be the Linux operating system. It already works on the command line, which makes things a bit easier and will have all of the protection that you need as well. And so, we are going to spend a bit of our time taking a closer look at how the Linux system is going to be able to help us out with some of the hacking we want to accomplish.

There are a lot of reasons that hackers are going to enjoy working with Linux over some of the other operating systems that are out there. The first benefit is that it is open source. This means that the source code is right there and available for you to use and modify without having to pay a lot of fees or worry that it is going to get you into trouble. This open-source also allows you to gain more access to it, share it with others and so much more. And all of these can be beneficial to someone who is ready to get started with hacking as well.

The compatibility that comes with Linux is going to be beneficial for a hacker as well. This operating system is going to be unique in that it is

going to help us support all of the software packages of Unix and it is also able to support all of the common file formats that are with it as well. This is important when it comes to helping us to work with some of the hacking codes that we want to do later on.

Linux is also designed to be fast and easy to install. If you took a look at the second chapter in this guidebook, you might have noticed that there are a number of steps that we had to go through in order to get started. But when compared to some of the other operating systems this is not going to be that many and it can really help you to get the most out of this in as little time as possible.

You will quickly notice that most of the distributions that you are able to do with Linux are going to have installations that are meant to be easy on the user. And also, a lot of the popular distributions of Linux are going to come with tools that will make installing any of the additional software that you want as easy and friendly as possible too. Another thing that you might notice with this is that the boot time of the operating system of Linux is going to be faster than what we see with options like Mac and Windows, which can be nice if you do not want to wait around all of the time.

When you are working on some of the hacks that you would like to accomplish, the stability of the program is going to matter quite a bit. You do not want to work with a system that is not all that stable, or that is going to fall apart on you in no time. Linux is not going to have to go through the same periodic reboots like others in order to maintain the level of performance that you would like and it is not going to slow down or freeze up over time if there are issues with leaks in the memory and more. You are

also able to use this operating system for a long time to come, without having to worry about it slowing down or running into some of the other issues that the traditional operating systems will need to worry about.

For someone who is going to spend their time working with ethical hacking, this is going to be really important as well. It will ensure that you are able to work with an operating system that is not going to slow down and cause issues with the protections that you put in place on it. And you will not have to worry about all of the issues that can come up with it being vulnerable and causing issues down the line as well. It is going to be safe and secure along the way, so that you are able to complete your hacks and keep things safe, without having to worry about things not always working out the way that we would hope.

Another benefit that we will spend a bit of time on is how friendly the Linux network is overall. As this operating system is an option that is open source and is contributed by the team over the internet network, it is also able to effectively manage the process of networking all of the time. And it is going to help with things like commands that are easy to learn and lots of libraries that can be used in a network penetration test if you choose to do this. Add on that the Linux system is going to be more reliable and it is going to make the backup of the network more reliable and faster and you can see why so many users love to work with this option.

As a hacker, you will need to spend some of your time multitasking to get all of the work done. A lot of the codes and more that you want to handle in order to do a hack will need to have more than one thing going at a time,

and Linux is able to handle all of this without you having to worry about too much going on or the computer freezing upon you all of the time.

In fact, the Linux system was designed in order to do a lot of things at the same time. This means that if you are doing something large, like finishing up a big printing job in the background, it is not really going to slow down some of the other work that you are doing. Plus, when you need to handle more than one process at the same time, it is going to be easier to do on Linux, compared to Mac or Windows, which can be a dream for a hacker.

You may also notice that working with the Linux system is a bit different and some of the interactions that you have to take care of are not going to be the same as what we found in the other options. For example, the command-line interface is going to introduce us to something new. Linux operating systems are going to be specifically designed around a strong and highly integrated command-line interface, something that the other two operating systems are not going to have. The reason that this is important is that it will allow hackers and other users of Linux to have more access and even more control, over their system.

Next on the list is the fact that the Linux system is lighter and more portable than we are going to find with some of the other operating systems out there. This is a great thing because it is going to allow hackers with a method that will make it easier to customize the live boot disks and drives from any distribution of Linux that they would like. The installation is going to be fast and it will not consume as many resources in the process. Linux is light-weight and easy to use while consuming fewer resources overall.

The maintenance is going to be another important feature that we need to look at when we are trying to do some ethical hacking and work with a good operating system. Maintaining the Linux operating system is going to be easy to work with. All of the software is installed in an easy manner that does not take all that long and every variant of Linux has its own central software repository, which makes it easier for the users to search for their software and use the kind that they would like along the way.

There is also a lot of flexibility when it comes to working with this kind of operating system. As a hacker, you are going to need to handle a lot of different tools along the way. And one of the best ways that we are able to do this is to work with an operating system that allows for some flexibility in the work that we are doing. This is actually one of the most important features in Linux because it allows us to work with embedded systems, desktop applications and high-performance server applications as well.

As a hacker, you want to make sure that your costs are as low as possible. No one wants to get into the world of ethical hacking and start messing with some of those codes and processes and then find out that they have to spend hundreds of dollars in order to get it all done. And this is where the Linux system is going to come into play. As you can see from some of our earlier discussions of this operating system, it is going to be an open-source operating system, which means that we are able to download it free of cost. This allows us to get started with some of the hacking that we want to do without having to worry about the costs.

If you are working with ethical hacking, then your main goal is to make sure that your computer and all of the personal information that you put into it is going to stay safe and secure all of the time. This is going to be a command-line to keep other hackers off and will make it so that you don't have to worry about your finances or other issues along the way, either. And this is also where the Linux operating system is going to come into play to help us out.

One of the nice things that we are going to notice when it comes to the Linux operating system is that it is seen as being less vulnerable than some of the other options. Today, most of the operating systems that we are able to choose from, besides the Linux option, are going to have a lot of vulnerabilities to an attack from someone with malicious intent along the way.

Linux, on the other hand, seems to have fewer of these vulnerabilities in place from the beginning. This makes it a lot nicer to work with and will ensure that we are going to be able to do the work that we want on it, without having a hacker getting. Linux is seen as one of the most secure out of all the operating systems that are available and this can be good news when you are starting out as an ethical hacker.

The next benefit that we are going to see when it comes to working with the Linux operating system over some of the other options, especially if you are a hacker, is that it is going to provide us with a lot of support and works with most of the programming languages that you would choose to work on when coding. Linux is already set up in order to work with a lot of the most

popular programming languages. This means that many options like Perl, Ruby Python, PHP< C++ and Java are going to work great here.

This is good news for the hacker because it allows them to pick out the option that they like. If you already know a coding language or there is one in particular that you would like to use for some of the hacking that you plan to do, then it is likely that the Linux system is going to be able to handle this and will make it easy to use that one as well.

If you want to spend some of your time working on hacking, then the Linux system is a good option. And this includes the fact that many of the hacking tools that we are working with are going to be written out in Linux. Popular hacking tools like Nmap and Metasploit, along with a few other options, are going to be ported for Windows. However, you will find that while they can work with Windows, if you want, you will miss out on some of the capabilities when you transfer them off of Linux.

It is often better to leave these hacking tools on Linux. This allows you to get the full use of all of them and all of the good capabilities that you can find with them, without having to worry about what does and does not work if you try to move them over to a second operating system. These hacking tools were made and designed to work well in Linux, so keeping them there and not trying to force them into another operating system allows you to get the most out of your hacking needs.

And finally, we are able to take a quick look at how the Linux operating system is going to take privacy as seriously as possible. In the past few years, there was a lot of information on the news about the privacy issues

that would show up with the Windows 10 operating system. Windows 10 is set up to collect a lot of data on the people who use it the most. This could bring up some concerns about how safe your personal information could be.

This is not a problem when we are working with Linux. This system is not going to take information, you will not find any talking assistants to help you out and this operating system is not going to be around, collecting information and data on you to have some financial gain. This all can speak volumes to an ethical hacker who wants to make sure that their information stay safe and secure all of the time.

As you can see here, there are a lot of benefits that are going to show up when it is time to work with the Linux system. We can find a lot of examples of this operating system and all of the amazing things that it is able to do, even if we don't personally use it on our desktop or laptop. The good news is that there are a lot of features that are likely to make this operating system more effective and strong in the future, which is perfect when it comes to doing a lot of tasks, including the hacking techniques that we talked about in this chapter.

Conclusion

Thank you for making it through to the end of *Linux for Beginners:An Introduction to Linux Programming Basics for Hackers, Its Operating System, Command-Line and Networking, Including Effective Strategies, Tips and Tricks to Learn How It Works*, let's hope it was informative and able to provide you with all of the tools you need to achieve your goals whatever they may be.

The next step is to get started with some of the work that we want to be able to work with when it is time to bring out the Linux operating system. In many personal computers, other options like Windows and Mac are going to be the main operating systems that we are able to work with. But there are many other applications out there that are going to rely on Linux and all of the neat features that come with this option as well. It is free to use, comes with fewer problems than some of the other operating systems and can really help us to get things done without worrying about viruses, malware and even ransomware along the way. With this in mind, we are going to spend some time in this guidebook looking at what the Linux system is able to do for us and why it is such a powerful option to rely on.

This guidebook spent some time going through the basics of the Linux system. There are so many things that we are able to do when it comes to working with this operating system and we are going to discuss the benefits

of working with this, why the costs are so low compared to other operating systems and some of the different distributions that we are able to work with as well.

But that is just the beginning to help us get our feet wet in the process. We are also going to spend some time looking at more about this as well. To start with, we are going to spend some time creating our VirtualBox so that we can use Linux when we would like, while still maintaining some of the other operating systems that we would like to use. Then we moved on to learning more about some of the commands that we can use in Linux, how to handle the Fish shell and even how to handle some of the protection and more that need to happen in order to make sure that your files and directories are not going to be corrupted in the process.

To finish off this guidebook, we spent a bit of time looking at a few other important things that can help us to get our work done as well. We spent some time looking at how to handle the text editors that we are able to work with, including some information on Nano and Vi so that you can write out some of the commands that you would like. And then, there was a discussion on how we are able to use the Linux operating system as our number one tool to handle most of the work that we want to do with hacking.

There are a lot of great operating systems out there that we are able to work with as well. Windows and Mac can provide us with some great options as well. But if you are looking for an option that is going to have a lot of power and great features and will be open-sourced and not cost what the others do, then the Linux operating system is the best option for you to

choose from. When you are ready to learn more about the Linux system, make sure to read through this guidebook to help you get started.

Finally, if you found this book useful in any way, a review on Amazon is always appreciated!

Kali Linux

A Comprehensive Step-by-Step Beginner's Guide to Learn the Basics of Cybersecurity and Ethical Computer Hacking, Including Wireless Penetration Testing Tools to Secure Your Network

Table of Contents

Introduction

Chapter 1: Introduction to Kali Linux
- History of Kali Linux
- Tool categories in Kali Linux
- The Lifecycle for Penetration Testing
- General Penetration Testing Framework
- Let us look at the Ethics
- Terminologies

Chapter 2: The Basics of Kali Linux
- Downloading Kali
- Installation of Kali Linux on the Hard Drive
- First Time Booting of Kali Linux
- Setting the Defaults
- Initial Network Setup
- Why You Should Use Kali Linux
- The Terminal
- Basic Commands in Linux
- Finding Files
- Modify Files and Directories
- Removing a Directory
- Searching for tools/packages
- Adding Softwares
- Removing Softwares
- Updating Packages
- Upgrading Packages

Chapter 3: The Hacking Process
- Reconnaissance
- Enumeration
- Scanning
- Port Scanning
- Vulnerability Scanning
- Gaining Access

Maintaining Access
Rootkits
Clearing Tracks
Deleting Evidence
Chapter 4: Wireless Network Hacking
Wireless Hacking
Wireless Network attacks
WEP
WPA
How to perform MAC spoofing
Transmissions
Access Points
Devices
The Users
Chapter 5: Uses and Applications of Kali Linux
Penetration testing
Espionage and military
Chapter 6: Introduction to Cybersecurity
Introduction
Confidentiality, Integrity and Availability
Encryption
Backup and Redundancy
Chapter 7: Network Scanning and Management
Introduction
Network Scanning
Manipulating the Domain Name System (DNS)
Basic Wireless Commands
Detecting and Connecting to Bluetooth
Chapter 8: Web Security
Web Security
Common website security threats
How to safeguard your website
Conclusion

Introduction

Congratulations on purchasing *Kali Linux*: *A Comprehensive Step-by-Step Beginner's Guide to Learn the Basics of Cybersecurity and Ethical Computer Hacking, Including Wireless Penetration Testing Tools to Secure Your Network,* and thank you for doing so. The book covers the numerous tools in Kali Linux that you can use for performing penetration tests. You will also be able to learn the operations of the various utilities in this Debian distribution. To use this book effectively, you will require prior knowledge of basic Linux administration, computer networking and the command utilities but on a minimum. This will help you to comprehend the various subjects that have been covered herein.

You will get to know how hackers are able to gain access to your systems and the methods they use to steal information. Furthermore, you will also learn the countermeasures required to safeguard yourself against the numerous hacking techniques. To this end, the books cover topics that include: an Introduction to Kali Linux, The Basics of Kali Linux, The Hacking Process, Wireless Network Hacking, Uses and Applications of Kali Linux, Introduction to Cybersecurity
Network Scanning and Management and some basics on Web Security you will need to know in your journey to be a professional hacker.

By the time you flip the last page of this book you will have mastered both theoretical and practical concepts on the basic techniques that you require to become a hacker. You will have the techniques needed for penetration of

computer networks, computer applications alongside computer systems. Let me say that we have numerous books that cover this topic, but you have decided to pick this one up. Many thanks for that. No efforts have been spared in ensuring that the content in this book is relevant and refreshing to you. Have fun reading!

Chapter 1: Introduction to Kali Linux

In this chapter you will be introduced to a diverse area of ethical penetration testing. It is also referred to as ethical hacking and is defined as a technical

procedure and methodology which gives professional hackers a platform to simulate the techniques and actions that real-life hackers would use in the exploitation of an information system or a computer network. We are going to learn the steps that are usually followed by the penetration tester right from the understanding and analysis of a select target to the actual break-in. The book also covers topics dealing with the numerous tools that are used in the penetration testing exercise. These are briefly introduced in this chapter but will be covered in depth in chapter 4. The reader will get to understand the practical applications of Kali Linux in the real world besides knowing how to download and install this distribution of Linux. So, let us get into it without further ado.

History of Kali Linux

Offensive Security is the company behind this wonderful distribution. Kali Linux is the company's latest release. Kali is a live disk security distribution having over 300 penetration testing and security tools. If you have prior experience with the operating system, you may have noticed that the tools have been categorized into groups that are commonly utilized by penetration testers and any other entities doing the assessment of information systems. Kali Linux utilizes Debian 7.0 distribution as its base, unlike the earlier distributions that were released by Offensive Security. The operating system is of the same lineage as its predecessor, Backtrack Linux. It is worth noting that it is also supported by the same team.

The name change to Kali Linux, according to Offensive Security, implies that this operating system is a total rebuild of the Backtrack distribution. The major improvements that were made meant that it was not just a new

version of Backtrack but a new operating system altogether. Going down memory lane, you will remember that Backtrack itself, just like Kali, was an upgrade that was derived from White Hat and SLAX, abbreviated as WHAX alongside Auditor. Technically speaking, Kali is the most recent incarnation of the information security industry penetration and auditing assessment tools.

Tool categories in Kali Linux

Kali Linux comes prepackaged with plenty of tools we can use for carrying out penetration testing. As we have said previously, the tools in Kali Linux are categorized in a fashion that helps with the penetration testing exercise. Below are the broad categories:

1) **Information gathering tools:** In this category, we have numerous tools that are used in the information gathering process. Normally, a penetration tester would be interested in information about DNS, operating systems, IDS/IPS, SSL, network scanning, routing, voice over IP, SMB, e-mail addresses, VPN, and SNMP.

2) **Vulnerability assessment tools:** Here, tools that are used in the scanning of vulnerabilities, in general, are located. We have tools that are utilized for the vulnerability assessment of the Cisco network and database servers. We also have several fuzzing tools in this category.

3) **Web applications:** Just like the name, tools in this category relate to web applications. They include database exploitation, content management system scanner, web vulnerability scanners, web crawlers, and web application proxies.

4) **Tools for password attacks:** Tools that you can use to carry out both online and offline password attacks are found under this category.

5) **Exploitation tools**: You will find tools for the exploitation of the vulnerabilities unearthed from a selected target environment. Here, you will get exploitation tools you can use for databases, the Web, and the network. Also, under this category, you will find tools for carrying out social engineering attacks. The tools will give the user information about the exploits carried out too.

6) **Tools for sniffing and spoofing:** The tools here are used for sniffing web traffic and the network traffic. We also have network spoofing tools, for example, Yersinia and Ettercap.

7) **Tools for maintaining access:** A penetration tester will use the tools found here to maintain their access to a target machine. Obviously, you require the highest level of privilege to install tools located in this category. We have tools that can be used for backdooring web applications and the operating system. Tools used for tunneling are also found in this category.

8) **Tools for reporting:** Tools that are used for documentation of the penetration testing methodology and the obtained results and recommendations are found in this category.

9) **System services:** We have numerous services which are necessary during the penetration testing exercise in this category. Examples

include: the Metasploit service, Apache service, SSH service, and MySQL service.

10) **Wireless attacks:** Here, we have tools for carrying out attacks on wireless devices, RFID/NFC and Bluetooth devices.

11) **Reverse engineering:** Tools in this category are normally used for debugging programs or carrying out disassembly of executable files.

12) **Stress testing**: If you want to carry out stress testing of your network, VOIP environment, wireless and Web, you will find all the tools relevant in this category.

13) **Hardware hacking:** If you are interested in working with Arduino and Android applications, all the tools you need are found here.

14) **Forensics:** The forensics category contains numerous tools normally utilized in digital forensics. Examples of forensics include the acquisition of hard disk images, carving of files and, more importantly, analyzing the image retrieved from the hard disk. To do these tasks properly, a user is required to go to the Kali Linux Forensics menu then select the No Drives or Swap Mount from the booting menu. This way, the operating system will not automatically mount the drives. This implies that the integrity of the drives will be maintained.

Hold onto this information for now as we will look at some of it in chapter 5.

The Lifecycle for Penetration Testing

Today, we have various lifecycle models of penetration testing that are being used. So far, the lifecycle and the methodology defined and used by the EC-Council Certified Ethical Hacker program is the one that is widely used. This penetration testing life cycle is made up of five phases, including Reconnaissance, Scanning, Gaining Access, Maintaining Access and finally Covering Tracks in that order. Later in the book, we will look at each of the stages above in detail.

General Penetration Testing Framework

We have said before that Kali Linux provides us with the versatility we need in the process of penetration testing and security assessment from the numerous tools it possesses. A penetration tester who does not follow a proper framework is likely to get unsatisfactory results emanating from unsuccessful testing. This means that it is therefore essential for managers and technical administrators to ensure that the security testing is in harmony with a structured framework: the goal of the test is to provide useful findings.

What you are going to learn here is a general testing framework that is normally used by both the white box and black box approaches. From it, you will get an elementary understanding of the typical phases that a penetration tester or a security auditor should progress. The frameworks, however, need to be adjusted appropriately basing on the target being assessed. The following are steps that need to be followed so that the assessment procedure is successful.

- Scoping of the target
- Gathering Information
- Discovery of the Target
- Target Enumeration
- Mapping out Vulnerabilities
- Social engineering
- The exploitation of the Target
- Escalation of Privilege
- Maintenance of access
- Reporting and Documentation

1. Scoping of the Target

This is usually the first step prior to beginning the technical assessment of the security. It is essential that observations are carried out on the target network environment so that the scope is well understood. It is also possible to define the scope for a given set of entities or a single entity that is given to the auditor. Examples of typical decisions normally made in this step include;

- What element requires testing?

- How will it be tested?
- What are the parameters that will be applied when conducting the test?
- What are the limiting factors of the test process?
- How long will the test take?
- What objectives are intended to be achieved?

For any penetration testing exercise to be successful, the tester must have a good understanding of the technology being assessed, its basic operations together with the way it interacts with the network environment. What this means is that an auditor's knowledge is what determines the success of the penetration testing procedure.

2. Information gathering

After scoping has been done, the next phase is the reconnaissance phase. Here, the penetration tester will make use of resources that are available publicly to get a better understanding of their target. One can get valuable information from sources on the Internet, which include:

- Social networks
- Articles
- Forums
- Blogs
- Bulletin boards
- Commercial or non-commercial websites
- Newsgroups
- Search engines, for example, MSN Bing, Google, among others.

Additionally, Kali Linux has several tools that you can use to get a target's network information. The tools use crucial data mining techniques for gathering information from DNS servers, e-mail addresses, traceroutes, phone numbers, Whois database, personal information, and user accounts. Chances of having a successful penetration test increase with the amount of information that is gathered.

3. Target discovery

Here, key activities are the identification of the network status of selected targets, its OS and, if possible, the target's network architecture. Such information gives a penetration tester a comprehensive outlook of the interconnected devices or current technologies in the network. That means that they will be able to enumerate the numerous services running within the network. It is possible to do all this (determination of hosts on the network that are live, the running OS on the hosts and the characterization of each of them based on their roles in the network system) using the Kali Linux advanced network tools. The detection techniques employed by these tools can either be active or passive. This is done on top of network protocols and can be manipulated in a fashion that will yield useful information. An example of this information is the OS fingerprinting.

4. Target Enumeration

This phase advances the previous efforts by finding open ports on the systems being targeted. After the identification of open ports, enumeration of the ports will be done for the running services. Employing port scanning techniques like stealth, full-open, and half-open scan can assist a hacker, or a penetration tester checks the visibility of ports. This is possible for hosts that are behind an Intrusion Detection System or a firewall. To help penetration testers or hackers discover existing vulnerabilities in a target

network's infrastructure, an investigation of the services which are mapped to the open ports can be done. This means that we can use target enumeration as a platform for unearthing vulnerabilities present in the various devices on the network. Through the vulnerabilities, one can penetrate the network. A security auditor can utilize Kali Linux's automated tools to do target enumeration.

5. Vulnerability mapping

By now, we will be having enough information about the target network. We will now need to analyze the identified vulnerabilities basing on the services and ports we have discovered. We have automated vulnerability assessment tools for applications and the network in Kali Linux that can help us achieve the objectives of this phase. It is also possible to do vulnerability mapping manually. The only downside is that it requires expert knowledge and consumes plenty of time. The best approach to this is to combine the two so that a security auditor can have a clear vision that will enable them to investigate vulnerabilities that are either known or unknown in the network systems.

6. Social engineering

Social engineering is a type of attack which uses human beings as attack vectors. In most information security configurations, human beings are regarded as the weak link through which an attacker can gain access to a system. An attacker can penetrate a target network and execute a malicious code that will do some damage and, in some cases, create a backdoor for future use. All this will have been made possible through deceiving the

people in charge of or those using a given network. Social engineering can be of different forms. For instance, an attacker using a phone can pretend to be a network administrator prompting a user to disclose their account information. Another form of social engineering is an e-mail phishing scam, which is used by malicious users to steal the account details of your bank. Physically, a person can imitate a legitimate user to gain access to a physical location. This is also social engineering. From these examples, we can see that the possibilities for achieving a required goal are immense. To make any penetration testing exercise successful, it is important that the tester or attacker takes time to understand human psychology as it is a skill that will help them improvise accordingly in their targeting. Note that most countries have laws regulating this, and as such, it is good to know the laws before attempting anything lest you end up in jail.

7. Target exploitation

After we have studied the vulnerabilities we have uncovered, we can go ahead and penetrate our target based on the available types of exploits. Most of the time, modifications or additional research on existing exploits are needed to ensure the exploits work as intended. The task is, of course, daunting. However, Kali Linux comes prepackaged with advanced exploitation tools that can help in the simplification of the exercise. Further, a tester is at liberty to employ client-side exploitation tactics in addition to some little social engineering to enable them assume control of a target system. A keen reader should, by now, see that this phase concentrates more on the process of target acquisition. Target exploitation encompasses three key areas. These are pre-exploitation, exploitation, and post-exploitation activities.

8. Privilege escalation

After target acquisition, the penetration exercise will be deemed successful. The penetration tester or auditor will now be able to roam in the system freely based on their access privileges. Using local exploits matching the environment of the system, a tester can escalate these privileges. Once these exploits are executed, a hacker or a penetration tester will now be able to get system-level or super-user privileges. From here onwards, a tester can carry out additional attacks on the local network systems. Based on a target's scope, this process can either be non-restricted or restricted. It is also possible to get more information regarding a compromised target through cracking passwords to various services, network traffic sniffing, and employing spoofing tactics on local networks. This implies that the main objective of privilege escalation is to enable one to acquire the highest-level access to the targeted system.

9. Maintaining access

A penetration tester, in some instances, can be requested by a client to maintain their access in the system for a specified period. This can be used as a demonstration to the network managers to show how illegal access to the system can be done without the need for a penetration process again. Also, it serves to save resources, time and cost that is spent in gaining access to the system for purposes of assessing its security. One can choose to use secret tunneling methods that utilize proxy, protocols, or end-to-end connection strategies. This way, a tester can create backdoor access, which will assist them in maintaining their presence in a target system for as long as they are required to. This technique of accessing the system gives us an indication of how an attacker can keep their presence in a targeted system without raising suspicion.

10. Reporting and Documentation

A penetration testing exercise will not be complete if a presentation of disclosed vulnerabilities is not done. Verified and exploited vulnerabilities should be well documented, reported and presented. Ethically speaking, this is crucial as it will help the network and system administrators and managers to direct their resources towards sealing any security loopholes present in their infrastructure. The reports will have different outlooks based on the needs of the different contracting organizations. The customizations of the report will help technical staff and businesses get to know and analyze points of weaknesses existing in their IT infrastructure. In addition to that, the reports can be used in the comparison of the integrity of a target system after and before the penetration process.

Let us look at the Ethics

To ensure that everything remains legal, we have rules of engagement. These must be adhered to by the auditors and other information security professionals.

These rules describe the way the penetration testing should be given, the way testing is to be performed, the determination of legal negotiations and contracts, definition of the testing scope, test plan preparation, the process the test should follow, and the management of a reporting structure that is consistent. A keen examination is required to address each of these areas. The making of formal procedures and practices need to be adhered to

throughout the engagement period. These rules include but are not limited to, the following:

1. The test schedule should be chosen in a way that does not affect or interrupt the normal operation of a business. It is prudent to create a schedule that does not cover the typical working hours.

2. The rules governing the test process clearly outline a set of steps to be followed during the testing exercise. The organization's managers and technicians participate in the formulation of these rules for purposes of restricting the testing process with its environment and people.

3. It is forbidden to provide testing services to a client after hacking their systems prior to coming up with any formal agreement. This is akin to unethical marketing, and in some cases, it may lead to failure of the normal business operations and can cause one to face excruciating legal repercussions based on the country's rules and laws.

4. It is strictly prohibited to conduct a penetration test past the scope of testing or breaching the set limits without a clients' express permissions.

5. A legally binding contract should be agreed upon by parties involved so that it limits the liability of a job unless there is evidence of illegal activity. It must clearly state the conditions and terms of the test procedure, the emergency contact information, the description of work, and any conflicts of interest if present.

6. The scope of the penetration test should be clearly defined, indicating the contractual entities and any restrictions that have been imposed on them during the procedure.

7. On completion of the testing, reports and results must be presented in a consistent and clear fashion. It should include all the vulnerabilities that are known and unknown. Furthermore, it needs to be confidentially delivered to authorized personnel only.

Terminologies

In this book, we are going to encounter commonly used terms in the field of penetration testing. The terms are normally understood differently by members, technicians and professionals in the same field, and that is the reason we need a working definition to avoid any misunderstanding. Below are the terms and associated definitions we shall be using.

Penetration Testing

We define it as the process, methodology and procedures that are used in the attempt to bypass the safeguard mechanisms of the information systems, including overcoming the integrated security set up of that system. Normally, the entire process follows approved and specific guidelines. Penetration Testing is concerned with examining the administrative, technical, and operational controls and settings of a system. The testing assesses the security of a particular information system exactly as it is configured. The system administrators and staff of the targeted network may or may not know that such an exercise is happening.

Ethical Hacking

This is a professional penetration tester whose main job is to carry out an attack on the computer or network systems for an organization or a particular owner of the information system. In this book, you will note that Ethical Hacking and Penetration Testing are used interchangeably.

White Hat

This terminology is synonymous with computer security professional or an Ethical Hacker who is specialized in the security testing of information systems so as to provide security where it is lacking or improve it where it is possible.

Black Hat

This is a terminology used to describe a person who uses his IT skills for bypassing the security of information systems without permission. The intention of black hats is normally to commit computer crimes. Red Team members, together with Penetration Testers, normally employ techniques used by Black Hats in their work. This is to simulate the malicious fellows in security testing while they are carrying out legitimate tests or exercises.

Grey Hat

In life, we have the good guys, the bad guys and those who lie in between. In hacking, grey hats are those in the middle. Normally, they will try to circumvent the security features of an information system in most cases without prior permission. They do this normally to bring to light the discovered weaknesses to the system administrators. In most cases, they are

not after profit. What makes them illegitimate is the fact that they do not seek prior permission from the owners before carrying out their activities.

Vulnerability Assessment/Analysis

This is an exercise done to evaluate the security configurations of a system. The forms of the assessments that can be carried out comprise the evaluation of security patches that have been applied to a system and those that are missing. The team that carries out Vulnerability Assessment can either be external or it can be part of an organization's IT team.

Malicious User Testing

In this scenario, the assessor will act as if they were an insider acting maliciously. Of course, being an insider makes them a trusted entity. What happens is that the assessor will be given legitimate login credentials belonging to an authorized user; this will be a test account. They will then go ahead and use the credentials to try and circumvent laid down security measures. They can do this by modifying settings that are not supposed to be changed, viewing settings and documents that the account is not authorized to and escalating their permissions and privileges beyond the level the test account should have. In summary, a malicious user test attempts to simulates actions that a rogue insider can carry out using their trusted credentials.

Phishing

In this type of attack, attempts will be made to get the targeted entities to reveal personal information such as passwords, account numbers, and user names. Normally, this is done by the use of authentic-looking emails that

are fake. The emails can be from customer support staff, banks and corporations. A different type of phishing attack is where users are prodded to click on phony hyperlinks. This will make it possible for malicious codes to be installed on the target system without the owner's knowledge. Once this has been done, the malware can be used to attack other computers or for obtaining data stored on the computer. Phishing attacks are by nature, not directed to a specific target. Targets can be all the people in a mailing list or those whose email addresses have a specific extension, such as those with a "@kali.com" extension.

Spear Phishing

This is a type of phishing attack whereby the targets are specific. For instance,

An attacker can perform reconnaissance to discover email addresses of top-level management of an organization. They can go ahead then to carry out the phishing attack on only these individuals.

Dumpster Diving

In this technique, the penetration tester will make attempts to filter through a systems' discarded trash. This trash might be from any of the users and the system administrators. Any information obtained here will be of great help in understanding a particular target. A penetration tester might recover information detailing network diagrams, system settings and configurations, the hardware components and the software versions that are being used. On a good day, one might even get user credentials such as passwords and user names. Dumpster Diving is a term used to explain the process of entering a

large trash container. Also, garbage cans from small offices normally have some lucrative information.

LiveOS, Live Disk, Live CD

The terms above are used to refer to an optical disk containing a complete operating system. Live disks are a crucial asset to penetration testers and assessors since it is possible to modify them to suit the needs at hand. One can customize them to have specific settings, tools and software components. Many of the live disks in distributions are normally Linux based, although, over the years, we have had numerous Microsoft Windows versions being released. In most assessments, it is sufficient for an assessor to only bring with them a live disk. The systems under assessment can be directly booted to the live disk, effectively turning the information systems assets against the system itself.

Chapter 2: The Basics of Kali Linux

Downloading Kali

In the introduction, we pointed out that Kali Linux is a Linux distribution and can be downloaded as an ISO file. You will be required to download it from a different computer, after which you will burn it onto a disk before installation. You can download this interesting distribution of Linux from this link http://www.kali.org/downloads/. To know how to install it, you can get the documentation for configurations, advanced operations, and special cases on http://www.kali.org/official-documentation/. If you need any additional help, we have an active community where you can make any inquiries or you can help other members solve their problems. Offensive Security manages these community boards, and new users are required to register to enable them to obtain access.

The security company is the makers of Kali Linux. Occasionally, Offensive Security will provide messages pertaining to their products, community information and updates. When downloading Kali Linux, ensure that you select the proper architecture for your computer (either amd64564-bit or i386532-bit). I do not wish to talk about the images of Kali Linux in this book since that information is well captured in the links I have provided. Tap on the correct link to select and download the image. For those of you that are using Microsoft Windows, you will need to burn the image using

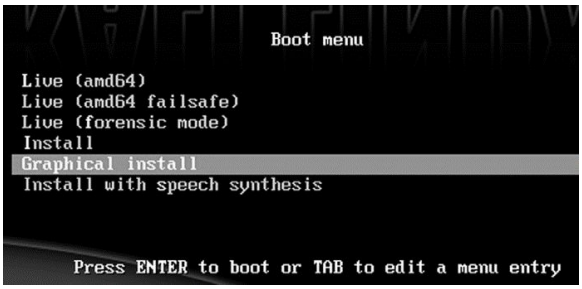
the Burn ISO or any other application (I can think of Rufus). Proceed with the burning process until it is complete. Similarly, Linux users can use a disk burning application (say K3b) to convert the ISO image.

Installation of Kali Linux on the Hard Drive

You are going to learn how to do a graphical and textual installation of this operating system. The graphical interface has been designed to be as simple as possible. You will be required to configure your Basic Input Output System
(BIOS) to boot from the optical disk you have created. First, load your optical disk or flash drive containing Kali onto the computer and start. For advanced users, there is an option of using virtualization technology like Oracle's VirtualBox or VMware's Player.

First Time Booting of Kali Linux

The screenshot below shows a computer that has successfully booted to the Kali Linux disk. 64-Bit Kali Linux version 1.0.5 has been used in this book. With time, you will observe that versions of Kali Linux that are downloaded at different times will appear different, albeit slightly. That aside, graphical installations are similar.



At http://www.kali.org/, you will find up to date guides for all the latest releases of Kali Linux. As such, it is important to check out this site before you carry out an installation. Kali Linux, besides being installed on a computer's hard drive, it can be run straight from the disk having the converted image. This is what we call a Live CD. This enables the operating system to boot. The tools that come with Kali will also execute. The only thing to note here is that the operating system from the live CD is nonpersistent. This terminology is used to mean that upon shutting down the computer, any memory, documents, saved settings and any other essential research or work is likely to be lost. A great way to learn Kali Linux is by running it in a nonpersistent state. Additionally, your current operating system will not be affected in any way. You can see that we have an option for installation with Speech Synthesis. We will not be going into the intricate details for that, but you should know that it is a recent upgrade feature to the Debian operating system and Kali. Users can control the installation procedure vocally if their hardware can support speech synthesis. How exciting! Like I have said before, let us concentrate on the graphical installation for
now. Using the directional keys, scroll and highlight Graphical Install and bang the Enter key.

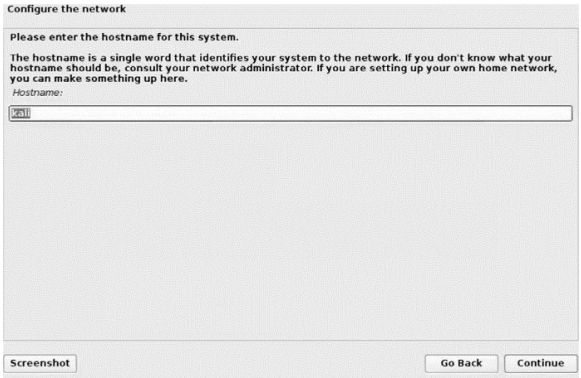
Setting the Defaults

You will be required to select default settings for your location, keyboard layout, and language in the next few screens. After you have made the appropriate selections, click on continue to proceed to the next step. You will notice various bars denoting progress on your computer's screen throughout the installation as the computer begins the actual installation of Kali. Picking the default settings is a good choice for most of the selection screens.

Initial Network Setup

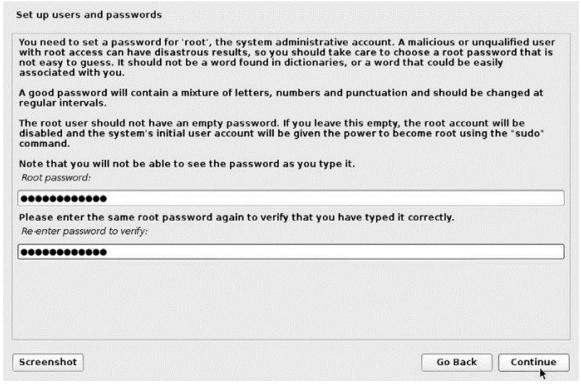
See the image below. In this stage, you will be required to do a basic configuration and an initial setup of your primary network interface card. Select a Hostname. Do this simply by typing in the provided box and hit the continue button to proceed. Make sure you pick a unique hostname to avoid having different computers with similar hostnames on the same network.

That will help to minimize networking complications. Once you are done choosing a hostname, hit the Continue button to proceed. On the next screen, you are going to provide a fully qualified domain name, FQDN. For most lab environments, this is not necessary unless you wish to join a domain environment. Let us leave it blank for now. We will click on the Continue button to move ahead.



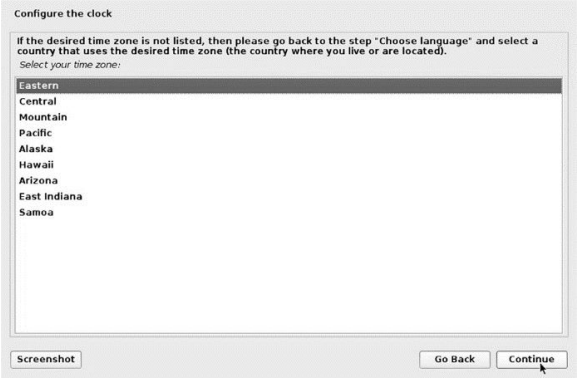
Setting Up Passwords

The next screen that comes up will prompt you for a root-level password. In Kali Linux, the default password is toor. I recommend that you create a new password that is strong, have no traceability to the user and that it should not be easy to guess. On keying in the password twice, tap the Continue button to move on to the next step. Are you still with me? Let us now configure the system clock.



Configuring the System Clock

You will be prompted to select a time zone of your choice, as shown in the figure below. Choose appropriately and then press the Continue button to proceed onto the next installation step.

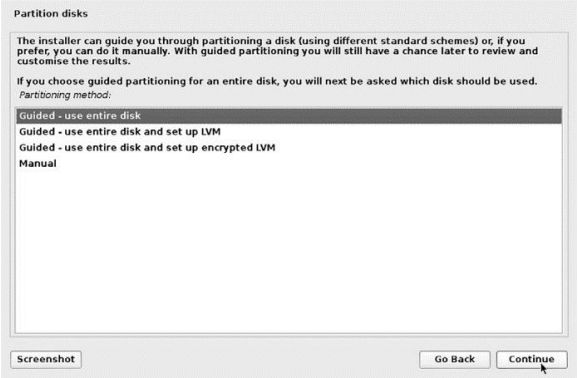


Configuration of the clock.

Partitioning Disks

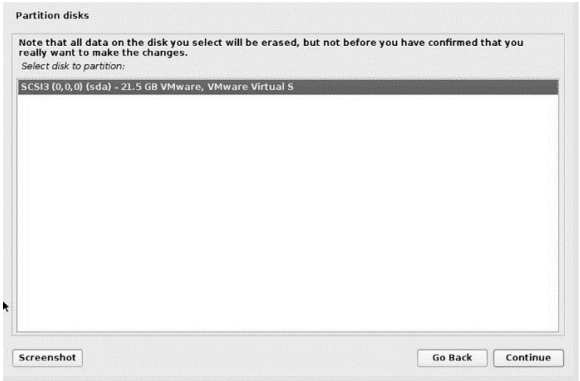
We have several ways of configuring partitions for setting up a Linux OS. We are going to focus on Guided Partitioning, which is the most basic installation. The figures below display the settings that are normally highlighted by default. You do not have to select anything till you reach the figure under partition disks - 5. All you need to do is click on the continue button until partitioning is complete. Let us take some time and understand what is happening at each step of the installation wizard.

Below, you will see the various options that you can choose for partitioning your computer's hard drives during the installation.



Partition disks - 1.

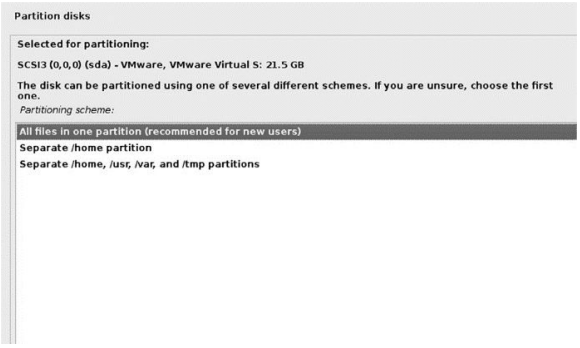
For laptop SD card or thumb drive installation, it is not recommended to use Logical Volume Management (LVM). Advanced users normally use LVM for managing many hard drives. The option that you should select is "Guided - user entire disk." Hit the Continue button to move onto the next step of the installation process. The figure below will indicate which drive has been picked for installation. Click on Continue to proceed.



Partition disks - 2.

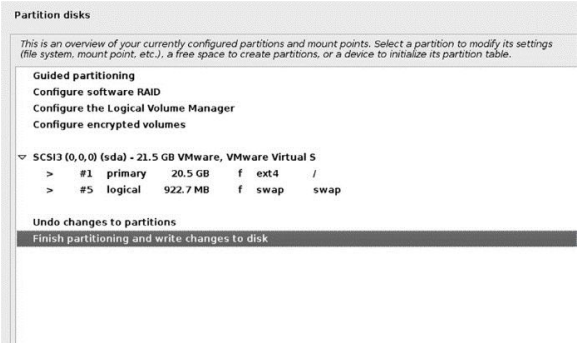
If you are a new Kali Linux user, select the option "All files in one partition (recommended for new users)." This is the best option for you. Hit the

Continue button to proceed with the installation.



Partition disks - 3.

Keep clicking on the continue button to advance the installation.

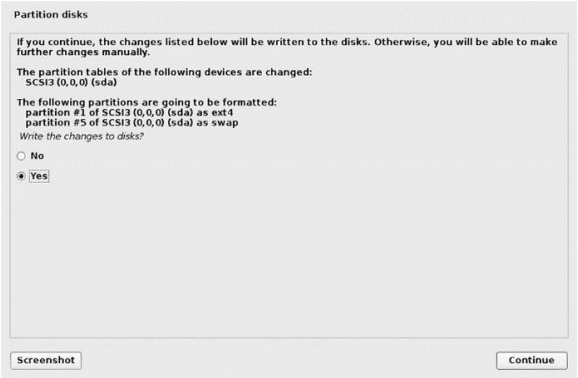


Partition disks - 4.

The wizard will take you through the above steps and present you with a screen for your review. Now, a partition having all the system, scripting, and user files, known as the primary partition, will be created as a single partition. A second partition will be made for swap space. This is a virtual memory in the system that is used for paging files to and from the computer's random-access memory and the central processing unit. It is recommended that all systems running Linux have a swap area. The

common practice is to configure the swap area be one and a half times or even equal to the amount of the computer's installed physical random-access memory (RAM).

You will come to a screen looking like this.



Partition disks - 5.

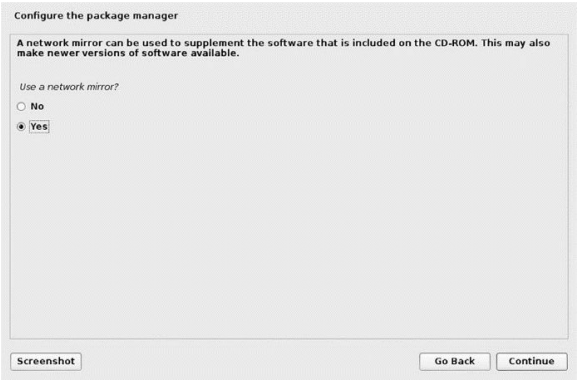
From the figure above, you will be asked to "Finish partitioning and write changes to disk." Pick the Yes option and click on the Continue button to proceed with the installation process. Take note that that will be the last chance you will have to review your partitioning options prior to the installation of the operating system on the hard drive. Should a need to amend the sizes of the partition arise in the future, it is still possible to do that. However, changing the partition sizes can destroy your operating system if it is not carried out properly.

Installation in progress.

The partitioning of the hard drive and installation will begin after you click continue (at the figure at partition disks – 5). The installation can take an hour or even a few minutes depending on your computer's hardware.

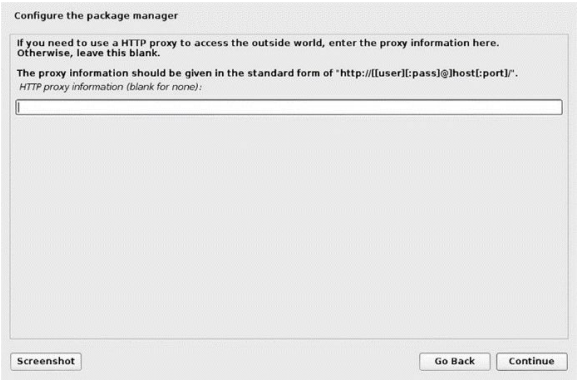
Setting Up the Package Manager

This is the update repository where your operating system will derive its security patches and updates from. As such, the package manager is very important in the functioning of the operating system. You can use the network mirror, which comes together with the Kali Linux image. It is recommended to use it since it contains the latest for package management sources. A "YES" option will be picked for you by default, as shown in the figure below. Proceed with the installation process by clicking on the Continue button.



Configuration of the package manager.

Suppose you are utilizing a proxy; you will need to input the configuration information on the next prompt the installation wizard will bring up. You can leave it blank as below. Hit the Continue button to proceed to the installation of the GRUB loader.

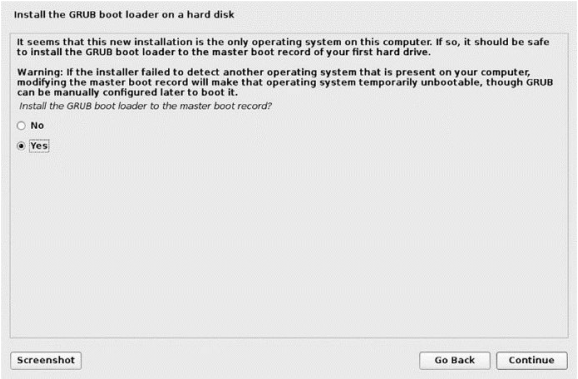


Configuring a proxy.

Install the GRUB Loader

GRUB is an abbreviation for Grand Unified Bootloader, and it is the main screen you will see each time you start the computer. GRUB provides a

platform where a user can verify specific settings during the booting up, make changes where it is necessary and adjust settings prior to the loading of the operating system. GRUB is highly recommended for most Linux installations even though there are advanced users who do not necessarily need it. The figure below indicates that “YES” has been picked for you to install the GRUB. To advance to the next installation stage, click on the Continue button.



Installing the GRUB loader.

Completing Installation for Kali Linux

Your installation will now be complete. Take out the optical disk or flash drive from the computer and reboot. The computer will prompt you to reboot. Select the Continue button to complete your installation. See the figure below. Upon rebooting, you will be met with a welcome screen requiring you to log in. Use the credentials you set up earlier. That will be it. Welcome to Kali Linux!

Completing the installation.

Why You Should Use Kali Linux

As we have said before, Kali Linux comes with just about every tool pre-installed that can be used for any of the above purposes. It is for this reason that Security Auditors, Forensics Investigators, Penetration Testers and Researchers prefer it.

Kali can be used in the breaking of WiFi networks, to hack websites and networks, to run Open Source Intelligence on an entity, among others. Kali Linux possesses tools that can be used for forensic investigation besides ethical hacking. This is becoming an equally essential branch of security that primarily collects evidence, analyze it and uses the results to backtrack Cyber Criminals. Forensic Investigation makes it possible to locate and eradicate malicious effects emanating from malicious activities. It also comes in handy in the calculation and management of loss that occurs after

a Cyber Attack. A key feature in Kali is the stealth Live mode mostly used in forensics and that it does not leave traces (fingerprints and footprints) on a host's system.

The Terminal

The very initial step in using Kali is to open the terminal, which is the command-line interface we'll use in this book. In Kali Linux, you'll find the icon for the terminal at the bottom of the desktop. Doubleclick this icon to open the terminal or press CTRLALTT. The terminal opens the command line environment, known as the shell, which enables you to run commands on the underlying operating systems and write scripts. Although Linux has many different shell environments, the most popular is the bash shell, which is also the default shell in Kali and many other Linux distributions. To change your password, you can use the command passwd.

Basic Commands in Linux

To begin, let's look at some basic commands that will help you get up and running in Linux.

- Finding Yourself with pwd

The command line in Linux does not always make it apparent which directory you're presently in, unlike that in Windows or macOS. To navigate to a new directory, you usually need to know where you are currently. The present working directory command, pwd, returns your location within the directory structure. Enter pwd in your terminal to see where you are:

```
kali >pwd
/root
```

In this case, Linux returned /root, telling me I'm in the root user's directory. And
because you logged in as root when you started Linux, you should be in the root user's directory too, which is one level below the top of the filesystem structure (/). If you're in another directory, pwd will return that directory name instead.

- Checking Your Login with whoami

In Linux, the one "all-powerful" superuser or system administrator is called root, and it has all the system privileges needed to add users, change passwords, change privileges and so on. Of course, you do not want just anyone to have the ability to make such changes; you want someone who can be trusted and has proper knowledge of the operating system. As a hacker, you usually need to have all those privileges to run the programs and commands you need, so you may want to log in as root. A Linux user can see which user they are logged in as using the "whoami" command as below:

```
kali >whoami
root
```

Here, the user is logged in as root.

- Navigating the Linux Filesystem

Navigating the filesystem from the terminal is an essential Linux skill. To get anything done, you need to be able to move around to find applications, files and directories located in other directories. In a GUI-based system, you can visually see the directories, but when you're using the command-line interface, the structure is entirely text-based and navigating the filesystem means using some commands.

- Changing Directories with cd

To change directories from the terminal, use the change directory command, cd. For example, here's how to change to the /etc. directory used to store configuration files:

```
kali >cd /etc
root@kali:/etc#
```

The prompt changes to root@kali:/etc, indicating that we're in the /etc. directory. We can confirm this by entering pwd

```
root@kali:/etc# pwd
/etc
```

To move up one level in the file structure (toward the root of the file structure, or /), we use cd followed by double dots (..), as shown here:

```
root@kali:/etc# cd ..
root@kali:/# pwd
/
root@kali:/#
```

This moves us up one level from /etc. to the /root directory, but you can move up as many levels as you need. Just use the same number of double dot pairs as the number of levels you want to move:

- You would use .. to move up one level.
- You would use .. .. to move up two levels.
- You would use .. .. .. to move up three levels, and so on.

So, for example, to move up two levels, enter cd followed by two sets of double dots with a space in between:

kali >cd .. ..

You can also move up to the root level in the file structure from anywhere by entering cd /, where / represents the root of the filesystem.

- Listing the Contents of a Directory with ls

To see the contents of a directory (the files and subdirectories), we can use the ls (list) command. This is very similar to the dir command in Windows.

```
kali >ls
bin   initrd.img      media      run      var
boot  initrd.img.old  mnt        sbin     vmlinuz
dev   lib             opt        srv      vmlinuz.old
etc   lib64           proc       tmp
home  lost+found      root       usr
```

This command lists both the files and directories contained in the directory. You can also use this command on any particular directory, not just the one you are currently in, by listing the directory name after the command; for example, ls /etc. shows what's in the /etc. directory. To get more information about the files and directories, such as their permissions, owner, size and when they were last modified, you can add the -l switch after ls (the l stands for long). This is often referred to as the long listing. See the example below:

```
kali >ls -l
total 84
drw-r--r--    1    root     root    4096    Dec    5  11:15    bin
drw-r--r--    2    root     root    4096    Dec    5  11:15    boot
drw-r--r--    3    root     root    4096    Dec    9  13:10    dev
drw-r--r--    18   root     root    4096    Dec    9  13:43    etc
--snip--
drw-r--r--    1    root     root    4096    Dec    5  11:15    var
```

- Getting Help

Nearly every command, application or utility has a dedicated help file in Linux that guides its use. For instance, if I needed help using the best wireless cracking tool, aircrack-ng, I could type the aircrack-ng command followed by the --help command:

kali >aircrack-ng --help

Note the double dash here. The convention in Linux is to use a double dash (--) before word options, such as help, and a single dash (-) before single letter

options, such as –h. When you enter this command, you should see a short description of the tool and guidance on how to use it. In some cases, you can use either -h or -? to get to the help file. For instance, if I needed help using the hacker's best port scanning tool, Nmap, I would enter the following:

```
kali >nmap -h
```

Unfortunately, although many applications support all three options, there is no guarantee of the application you are using will. So if one option refuses to work, please try another.

Finding Files

Until you become familiar with Linux, it can be frustrating to find your way around, but knowledge of a few basic commands and techniques will go a long way toward making the command line much friendlier. The following commands help you locate things from the terminal.

- Searching with locate

Probably the easiest command to use is locate. Followed by a keyword denoting what it is you want to find, this command will go through your entire filesystem and locate every occurrence of that word. To look for aircrack-ng, for example, enter the following:

```
kali >locate aircrack-ng
/usr/bin/aircrack-ng
/usr/share/applications/kali-aircrack-ng.desktop
/usr/share/desktop-directories/05-1-01-aircrack-ng.directory
--snip--
/var/lib/dpkg/info/aircrack-ng.mg5sums
```

The locate command is not perfect, however. Sometimes, the results of locate can be overwhelming, giving you too much information. Also, locate uses a database that is usually only updated once a day, so if you just created a file a few minutes or a few hours ago, it might not appear in this list until the next day. It's worth knowing the disadvantages of these basic commands so you can better decide when best to use each one.

- Finding Binaries with whereis

If you're looking for a binary file, you can use the whereis command to locate it. This command returns not only the location of the binary but also its source and main page if they are available. Here's an example:

```
kali >whereis aircrack-ng
aircarck-ng: /usr/bin/aircarck-ng /usr/share/man/man1/aircarck-ng.1.gz
```

- Finding Binaries in the PATH Variable with which

The which command is even more specific: it only returns the location of the binaries in the PATH variable in Linux. For example, when I enter aircrack-ng on the command line, the operating system looks to the PATH variable to see in which directories it should look for aircrackng:

kali >which aircrack-ng
/usr/bin/aircrack-ng

Here, which was able to find a single binary file in the directories listed in the PATH variable. At a minimum, these directories usually include /usr/bin, but may consist of/usr/sbin and maybe a few others.

- Performing More Powerful Searches with find

The find command is the most powerful and flexible of the searching utilities. It is capable of beginning your search in any designated directory and looking for several different parameters, including, of course, the filename but also the date of creation or modification, the owner, the group, permissions and the size.
Here is the basic syntax for find:

find directory options expression

- Filtering with grep

Very often, when using the command line, you may want to search for a particular keyword. For this, you can use the grep command as a filter to search for keywords. The grep command is often used when output is piped from one command to another.

```
kali >ps aux | grep apache2
root  4851 0.2 0.7 37548  7668 ?  Ss  10:14  0:00   /usr/sbin/apache2 -k start
root  4906 0.0 0.4 37572  4228 ?  S   10:14  0:00   /usr/sbin/apache2 -k start
root  4910 0.0 0.4 37572  4228 ?  Ss  10:14  0:00   /usr/sbin/apache2 -k start
--snip--
```

In the above example, the command will display all the services that are running and then pipe that output to grep. What grep does is it will search the received output for the keyword we asked it to look for. In our case, the keyword is apache2. Grep will go ahead and output only the relevant results. This command saves time.

Modify Files and Directories

After finding the directories and files you were looking for, you may need to carry out several operations on them. We are going to learn the creation of directories and files, copy files, rename files, plus delete the files and directories.

- Creating Files

There are many ways to create files in Linux, but for now, we will look at two simple methods. The first is the cat, which is short for concatenate, meaning to combine pieces (not a reference to your favorite domesticated feline). The cat command is generally used for displaying the contents of a file, but it can also be used to create small files. For creating bigger files, it's better to enter the code in a text editor such as vim, emacs, leafpad, gedit or kate and then save it as a file.

- Concatenation with cat

The cat command followed by a filename will display the contents of that file, but to create a file, we follow the cat command with a redirect, denoted with the > symbol, and a name for the file we want to create. Here is an example:

kali >cat > kalilinux
Hacking with Kali Linux!

- File Creation with touch

The second command for file creation is touch. This command was initially developed so a user could touch a file to change some of its details, such as the date it was created or modified. However, if the file does not already exist, this command creates that file by default. Let's create newfile using the touch command:

kali >touch newfile

Now when I then use ls –l to see the long list of the directory, I see that a new file has been created named newfile. Note that its size is 0 because there is no content in the newfile.

- Creating a Directory

The command for creating a directory in Linux is mkdir, a contraction of make directory. To create a directory named newdirectory, enter the following command:

```
kali >mkdir newdirectory
```

To navigate to this newly created directory, do enter this:

```
kali >cd newdirectory
```

- Copying a File

To copy files, we use the cp command. This creates a duplicate of the file in the new location and leaves the old one in place. Here, we are going to create the file oldfile in the root directory with touch and copy it to /root/newdirectory, renaming it in the process and leaving the original oldfile in place:

```
kali >touch oldfile
kali >cp oldfile  /root/newdirectory/newfile
```

Renaming the file is optional and is done simply by adding the name you want to give it to the end of the directory path. If you don't rename the file when you copy it, the file will retain the original name by default. When we then navigate to newdirectory, we see that there is an exact copy of oldfile called newfile:

kali >cd newdirectory
kali >ls
newfile oldfile

- Renaming a File

Unfortunately, Linux doesn't have a command intended solely for renaming a file, as Windows and some other operating systems do, but it does have

the mv (move) command. The mv command can be used to move a file or directory to a new location or to give an existing file a new name. To rename newfile to newfile2, you would enter the following:

```
kali >mv newfile newfile2
kali >ls
oldfile newfile2
```

Now when you list (ls) that directory, you see newfile2 but not newfile, because it has been renamed. You can do the same with directories.

- Removing a File

To remove a file, you can use the rm command, like so:

kali >rm newfile2

If you now do a long listing on the directory, you can confirm that the file has been removed.

Removing a Directory

The command for removing a directory is similar to the rm command for removing files but with dir (for directory) appended, like so:

```
kali >rmdir newdirectory
rmdir:failed to remove 'newdirectory': Directory not empty
```

It is important to note that rmdir will not remove a directory that is not empty but will give you a warning message that the “directory is not empty,” as you can see in this example. You must first remove all the contents of the directory before removing it. This is to stop you from accidentally deleting objects you did not intend to delete. If you do want to remove a directory and its content all in one go, you can use the -r switch after rm, as shown below:

kali >rm -r newdirectory

Just a word of caution, though: be wary of using the -r option with rm, at least at first, because it is straightforward to remove valuable files and directories by mistake. Using rm -r in your home directory, for instance, would delete every file and directory there, that is certainly not what you were intending.

Searching for tools/packages

Before you download a software package, you can check whether the package you need is available from your repository, which is a place where your operating system stores information. The apt tool has a search function that can check whether the package is available. The syntax is straightforward:

```
apt-cache search keyword
```

Note that we use the apt-cache command to search the apt cache or the place it stores the package names. So if you were searching for the intrusion

detection system Snort, for example, you would enter the command shown below.

```
kali >apt-cache search snort
fwsnort - Snort-to-iptables rule translator
ippl - IP protocols logger
--snip--
snort - flexible Network Intrusion Detection System
snort-common - flexible Network Intrusion Detection System - common files
--snip--
```

As you can see, many files have the keyword snort in them, but near the middle of the output, we see snort – flexible Network Intrusion Detection System. That is what we are looking for.

Adding Softwares

Now that you know the snort package exists in your repository, you can use apt-get to download the software. To install a piece of software from your operating system's default repository in the terminal, use the apt-get command, followed by the keyword install, and then the name of the package you want to install. The syntax looks like this:

apt-get install packagename

Let us try this out by installing Snort on your system. Enter apt-get install snort as a command statement, as shown below.

```
kali >apt-get install snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
snort-doc
The following NEW packages will be installed:
snort
--snip--
Install these packages without verification [Y/n]?
```

The output you see tells you what is being installed. If everything looks correct, go
ahead and enter Y when prompted, and your software installation will proceed.

Removing Softwares

When removing software, use apt-get with the remove option, followed by the name of the software to remove. An example is listed below.

```
kali >apt-get remove snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer
required:
  libdaq0 libprelude2 oinkmaster snort-common-libraries snort-rules-default
--snip--
Do you want to continue [Y/n]?
```

Again, you will see the tasks being done in real-time, and you will be asked whether you want to continue. You can enter Y to uninstall, but you might want to keep Snort since we will be using it again. The remove command does not remove the configuration files, which means you can reinstall the same package in the future without reconfiguring. If you do want to remove the configuration files at the same time as the package, you can use the purge option, as shown below.

```
kali >apt-get purge  snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdaq0 libprelude2 oinkmaster snort-common-libraries snort-rules-default
--snip--
Do you want to continue [Y/n]?
```

Enter Y at the prompt to continue the purge of the software package and the configuration files. To keep things small and modular, many Linux packages are broken into software units that many different programs might use. When you installed Snort, you installed several dependencies or libraries with it that Snort requires so that it can run. Now that you are

removing Snort, those other libraries or dependencies are no longer needed, so they are removed, too.

Updating Packages

Software repositories will be periodically updated with new software or new versions of existing software. These updates do not reach you automatically, so you need to request them to apply these updates to your system. Updating is different from upgrading: updating updates the list of packages available for download from the repository, whereas upgrading will upgrade the package to the latest version in the repository. You can update your system by entering the apt-get command, followed by the keyword update. This will search through all the packages on your system and check whether updates are available. If so, the updates will be downloaded. See the example below.

```
kali >apt-get update
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling InRelease [30.5kb]
Get:2 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 Packages
[14.9MB]
Get:3 http://mirrors.ocf.berkeley.edu/kali kali-rolling non-free amd64
Packages
[163kb]
Get:4 http://mirrors.ocf.berkeley.edu/kali kali-rolling/contrib amd64
Packages [107kB]
Fetched 15.2 MB in 1min 4s (236 kB/s)
Reading package lists... Done
```

The list of available software in the repository on your system will be updated. If the update is successful, your terminal will state Reading package lists... Done, as you can see above. Note that the name of the repository and the values, time, size and so on might be different on your system.

Upgrading Packages

To upgrade the existing packages on your system, use apt-get upgrade. Because upgrading your packages may make changes to your software, you must be logged in as root or use the sudo command before entering an apt-get upgrade. This command will upgrade every package on your system that apt knows about, meaning only those stored in the repository, as shown below. Upgrading can be time-consuming, so you might not be able to use your system for a while.

```
kali >apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Calculating upgrade... Done
The following packages were automatically installed and no longer required:
--snip--
The following packages will be upgraded:
--snip--
1101 upgraded, 0 newly installed, 0 to remove and 318 not upgraded.
Need to get 827 MB of archives.
After this operation, 408 MB disk space will be freed.
Do you want to continue? [Y/n]
```

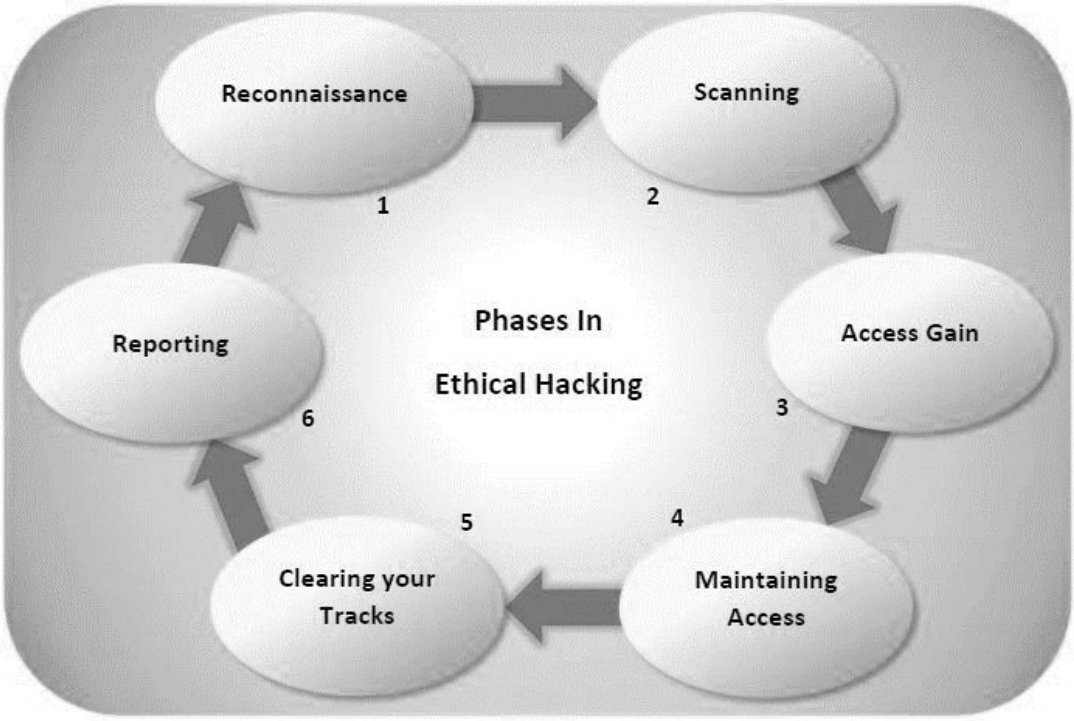
You should see in the output that your system estimates the amount of hard drive space necessary for the software package. Go ahead and enter Y if you want to continue and have enough hard drive space for the upgrade.

Chapter 3: The Hacking Process

In short, Ethical hacking, performed by white hat hackers, is a term used to describe defense hacking for companies and organizations, which involves the identification of potential threats on a computer or network.

Like all good projects, ethical hacking also has a set of distinct phases. It helps hackers to make a structured ethical hacking attack.Different security training manuals explain the process of ethical hacking in different ways, but in my experience, the entire process can be categorized into the following six phases:

1. Reconnaissance.
2. Scanning.
3. Access Gain.
4. Maintain Access.
5. Clearing your Tracks.
6. Reports.



Reconnaissance

What is Reconnaissance? From the dictionary meaning, it is a preliminary survey that is carried out to obtain information. An example is the exploratory surveys that militaries conduct on the territory belonging to the enemy. When it comes to cyber-security, Reconnaissance is a way of gathering information on a target using different techniques. When performing this exercise, there are three main information that is of interest to an ethical hacker;

1. The Network.
2. The Host.
3. Users/People involved.

Steps in Performing a Reconnaissance Exercise.

In ethical hacking, the first step is normally meant to help a penetration tester better understand their targets. This is done under a category that is collectively known as Information Gathering. Hereunder, we have something known as Reconnaissance, which we define as being a set of techniques and processes that are utilized in the discovery and collection of crucial information about a target. They include Scanning, Enumeration and Foot-printing. In an exercise meant for Reconnaissance, an ethical hacker tries to gather as much information about a target system as possible, following the seven steps listed below;

1. Collecting first information.
2. Determine a network's range.
3. Identification of active machines.
4. Discovering of Access Points and open ports that are available.
5. Operating System Fingerprinting.
6. Scanning for services running on various ports.
7. Network Mapping.

Reconnaissance is categorized into two major parts.

1. Active Reconnaissance: Active reconnaissance involves direct contact with your target's computer system to gain information, and information gotten directly is actually accurate. There is the risk of being caught in the

process of active reconnaissance without permission. But most hacking activities require active recon.
2. Passive Reconnaissance: In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

Enumeration

Enumeration, in the actual sense, is the complete listing of things in an orderly manner with regards to items in a collection. Enumeration is the act of making a list of policies, user accounts, shares and other resources. This step happens just before vulnerability assessment and after scanning. This helps the attacker put together the best strategy for gaining access. Enumeration can be used to gain information on:

1. Users and Groups
2. Networks and shared paths
3. Hostnames
4. Route Tables
5. Service Settings
6. SNMP port scanning
7. DNS Details Applications and Banners.

Enumeration can be done with the following tools. In the Windows Operating System, the use of many tools is done to enumerate NetBIOS names with commands like:
• Net accounts,
• Net config server,

• Net config workstation,
• Net view.

Scanning

This is a procedure that is used in the identification of services, active hosts and the ports that are used by the target application. Let us say you wish to unearth the vulnerabilities in a system, what you will need is a point you can attack in the System. In ethical Hacking, Network Scanning is employed to find out these points. These are points that Black Hats use to penetrate a system. After discovering these points, the relevant teams will then direct their efforts to improve the system. We know that all organizations have networks. They can either be internal or even connected to the internet. To hack these networks, you must first find a vulnerable point within them so that you can use it to carry out exploits. Network Scanning is the method we employ to help us discover such points within a network.

Network Scanning Objectives

1. It helps in the discovery of open ports, live computers or hosts and the IP address of the victim.
2. Network scanning makes it possible to identify the services which are running on the host computer.
3. It also aids in the discovery of the system architecture and the operating system of the target.
4. Scanning Live hosts enables us to unearth and mitigate vulnerabilities.

How is Network Scanning different from Reconnaissance?
To help you understand the difference between the two, I am going to use this analogy. Assume that you are commander in the army and you have been tasked together with your team to go and carry out an attack on a terrorist camp. We are going to assume that you already have an idea of the camps' location and the details about the vicinity of the camp. Now, this is information normally obtained through Reconnaissance. You will still be required to identify an entry point to the terrorist camp so that you can launch your attack. This is now what we are calling Network Scanning. We can confidently conclude that Reconnaissance is a technique you will use for gathering information to help you know more about your target. On the other hand, Network Scanning is a technique you will employ to help you locate possible vulnerable points within the network. It is through these points that one can penetrate a targeted network. Based on the information revealed by the scan, Network Scanning can be divided into two main categories:

- Port Scanning
- Vulnerability Scanning

Port Scanning

From the name, we can deduce that Port Scanning is a way of identifying active ports on the network. A Port Scanner works by transmitting requests from a client to the range of ports located on a network that they are targeting. The details about the ports will be saved and then a response will be transmitted back. This, good readers, is how active ports are found.

Upon acquiring a target's IP address (through scanning a victim organization's UDP and TCP ports), the hacker will proceed to map the organization's network under his/her grab.

Types of Port Scanning

SYNScan: In this mode of scanning, the TCP three-way handshake technique is not completed. Here, a hacker or penetration tester will send a victim the SYN packet. In case the response of an SYN/ACK frame is received, a connection will be completed by the target and the port will be able to listen. Receiving an RST from the target can mean that the port is not activated or it is closed. This type of scan has an advantage in the sense that only a few IDS systems will log this as a connection attempt or an attack.

XMASScan: The scan transmits a packet containing PSH (push), URG (urgent), and FIN (finish) flags. Suppose we have an open port; we do not expect a response; the target will respond with an RST/ACK packet if the port is closed. (RST=reset)

FINScan: This scan is almost similar to an XMAS scan with one exception. FINScan transmits packets with just the FIN (finish) flag. The scan does not have the other two flags (URG and PSH flags). The response is similar to that of XMAS scans. Also, the two scans have similar limitations.

IDLEScan: This kind of scan utilizes a spoofed IP for the transmission of a SYN packet to the target through the determination of the responses from

the port scan together with the IP header sequence number. The port is considered opened or closed based on the response of the scan.

Inverse TCP Flag Scan: In this case, a hacker will transmit TCP probe packets with a TCP flag (FIN, URG PSH) or with no flags. If there is no response, then it indicates that the port is open and RST means the port is closed.

ACK Flag Probe Scan: In this type of port scanning, an intruder will transmit TCP probe packets to a point where an ACK flag is set to a remote device that is used for the analysis of the header information. This information comprises of WINDOW and the TTL field. To know if the port is open or closed, one uses the RST packet. You can also use this scan for checking a target's filtering system.

Vulnerability Scanning

Essentially speaking, this is a type of Network Scanning that we use in our search for a network's weak points. Vulnerability Scanning unearths the vulnerabilities which can arise because of a misconfiguration of the network or due to poor programming. Before we go far, let us have a look at a few tools used for Network Scanning.

Tools for scanning networks and ports

Nmap: is utilized in the extraction of information, for instance, operating systems, type of packet filters/firewalls, live hosts on the network, services and the operating system versions.

Angry IP Scanner: this tool can be used to scan for IP addresses on systems available in each input range.

Superscan: this is a powerful tool developed by Mcafee. Besides being a TCP port scanner, it can also be used for pinging.

ZenMap: this scanner has a very powerful Graphical user interface tool that can help one detect the type of OS version, port scanning, OS, ping sweep, etc.

Net Scan Tool Suite Pack: this refers to a collection of different utilities and tools that are used for performing web rippers, port scans, mass emailers and flooding. Note that the tool is a trial version, but paid versions are also available.

Omnipeak and Wireshark are famous and powerful tools that are used for listening to network traffic. Both tools can be used as a network analyzer.

Countermeasures against scanning

1. System administrators can set up IDS and firewalls not only detect, but also block any probing attempts.
2. Employing custom rules which will lock down the network and bar any ports not wanted.
3. A user can run tools for port scanning so as to ascertain if the firewall detects any port scanning activities accurately.

4. Security Experts are required to make sure that there is a correct setting up of anti-spoofing and anti-scanners rules.
5. System and network managers need to ensure that the firewall firmware IDS and routers are up to date.

Gaining Access

Gaining access is by far the most critical phase of an attack. I am talking in terms of potential damage. Malicious actors do not always require to have access to a system to cause damage. For example, a denial-of-service attack can be carried out remotely with the potential to cause an abrupt termination of the services that are actively being executed on the target or in some cases, exhaust available resources. To stop a service, one can kill processes. This can be accomplished by the use of a logic/time bomb. Also, a reconfiguring and crashing of the system can achieve similar results. Network resources can be exhausted locally via the filling up outbound communication links. Such exploits can be done over a LAN or the Internet, locally, or offline as a deception or theft. Let us list some examples of these below:

- Session hijacking
- Buffer overflows that are Stack-based
- Denial-of-service and distributed denial-of-service

Sophisticated attackers normally carry out spoofing so that they can exploit a target's system by way of pretending to be different systems or strangers.

Using this approach, they can transmit a malformed packet having a bug. This bug will attempt to exploit vulnerabilities that are found in the target

system.

A technique known as packet flooding can be employed to remotely stop the availability of essential services. We have a different type of attack known as smurf attacks. These attacks attempt to elicit a response from the available network users. Their legitimate addresses will then be used to flood the victim. The success of gaining access to a target system by an attacker is heavily dependent on the following:

- The initial level of access gained.
- The level of skill of the attacker and
- The configuration and architecture of the target system.

The most damaging type of denial-of-service attack is the distributed denial-of-service attack. This happens when an attacker employs the use of zombie software that is spread over many machines on the Internet to initiate a coordinated large-scale denial of services.

Maintaining Access

After a hacker gains access to his target system, he/she will need to dedicate their efforts to ensure their boat remains afloat, metaphorically speaking. The attacker can decide to exploit the hijacked system while being in stealth mode, use it as a launching pad for attacks such as DDoS or spam campaigns or use it for scanning and exploiting other systems. All these actions can be damaging. Let me show you a practical example. A hacker

can create a sniffer to help them intercept all network traffic (both inbound and outbound). Part of the traffic can include the telnet sessions with other systems and file transfer protocols to enable them to send the captured data to any destination. Those who do not wish to be detected will be required to take steps that will help to conceal their presence. We have many techniques to do this. The preferred method is where the hacker installs hidden infrastructure based on covert channels, rootkits, Trojan horses and backdoors to enable them to have unfettered access to those systems.

Tools and Methods

A Trojan or backdoor is one such way to establish quick access to a system that has already been breached. A Trojan horse allows a hacker application-level access. The downside to this is that the Trojans need to be installed locally on a target system. In systems running Windows, it is possible for Trojans to install themselves as a service. After that, they will have administrative access. This means that they can run as a local system. A malicious individual can use these Trojans to steal credentials, passwords and any other sensitive information on the system. As the case with remote access Trojans, the backdoors attackers normally install come with inbuilt download and upload functionality. This technique relies on port 80 in the case of HTTP, 443 for HTTPS and port 53 for DNS for covering up their traffic.

A Covert Channel

This is a scenario where secret communication tunnels are used for transmitting data. Examples of such paths include HTTP tunnels, DNS tunnels, ICMP tunnels and VoIP. Take note that the covert channels we have mentioned can be used for transporting encrypted data as well. Detection of

covert channels is possible. Only that it requires substantial efforts on the victim's part. There are indicators of anomalies in the traffic going out, such as protocol analysis, network signatures and flow data analysis. These require special tools to come across. Take note that the detection of a covert channel is one thing, but blocking it is a different ball game. You can employ one or more of the following measures.

- Barring outbound ICMP at the corporate information border;
- Blocking requests that are DNS related to servers outside corporate networks. The requests can be allowed for internal DNS servers;
- HTTP tunnels disposing through the leveraging of Web proxies;
- You can schedule a delay in the delivery of voicemails in cases of exfiltration tunneling using VoIP RTR. This will allow for sending the voicemail to an audio processor for the examination of every packet to find any encoded data in the same way an antispam software works.

Rootkits

This is a malware that is highly adept at concealing itself from a computer system. It is this feature that distinguishes rootkits from other malware types. Their heightened capability to hide gives them the ability to circumvent security measures that have been put in place on the computer. The main idea behind their creation is the very fact that they are not easily detected by normal malware detection software. Normally, Trojan horses

are used to load rootkits beginning with “user” level access on the platform that is being targeted. Once in the target system, the rootkits will spy on login details such as passwords so that they can get “administrator” level access. Keen readers will say this is privilege escalation. That is correct. Despite this, the real specialty of the rootkits is to maintain access.

Rootkits will tend to hang around a targeted system slowly and progressively undermining it. This is unlike the norm with ordinary viruses that are designed to cause maximum damage in as little time as possible. The keyword here is ‘secrecy.’ For instance, keyloggers possessing rootkits are purposely built to capture all the words an unknowing victim keys in using their keypad. It will collect sensitive information for as long as it remains undetected. This makes identity theft highly probable. A good analogy is a parasite which, through various means, enters the body. It will stay dormant for a very long time. After it has mustered up enough energy to surmount over the body’s immune system, it will now go ballistic.

A computer system can be broken down into three basic layers. These are the operating system, the kernel and the hardware level. The kernel is the backbone of the operating system, essentially speaking. Many a time, low-priority processes are used by user-level rootkits to compromise the software tasked with safeguarding a computer. A dangerous and stealthier rootkit is the kernel-level rootkit. This is majorly due to the following reasons:

- Time and again, the removal of boot-level and kernel-level rootkits have been proven to be difficult.

- The rootkits that have made a residence in the kernel memory do not leave any traces on the hard disk normally. Additionally, these rootkits normally change parts of the disk, files and sometimes modify the kernel to enable them to become “reboot resistant.”
- Rootkits can camouflage their presence in cases where they make the addition of their code to sectors of the kernel;
- Kernel-level rootkits can run even before the operating system starts;
- This category of rootkits can bypass encryption through the creation of secret channels to allow them unfettered access to the compromised system.

Rootkits that are installed at the kernel level will acquire complete administrator access to the targeted systems. Rootkits normally create an access path right to the operating system level, unlike Trojan horses.

Removing rootkits

The typical security measures, for instance, antivirus software, cannot sufficiently deal with rootkits on their own. Alternatively, we have purpose-built programs such as Malwarebytes Anti-rootkit, TDSSKiller, Sophos Anti-Rootkit, and GMER that you can use to eradicate rootkits from your system. Note that, in some cases, the rootkit cannot be removed from your system for good. The programs above can only reduce the adverse effects that the rootkit leaves all over your system. In addition to using software to deal with rootkits, a user can also opt to initiate the clean slate procedure. Here, the important files are backed up, and a clean re-installation of the operating system is done. Normally, this will ensure that the rootkit is removed from your system. Again, this is not a guarantee that the removal

will be 100%. We have BIOS-level rootkits, which are rare but can survive the re-install. We will always have signs indicating a presence of rootkits in any system, no matter how hard they try to hide. This is major because they are designed to keep an ingress path for an attacker from outside.

Data Exfiltration

This can be described as an unauthorized transfer of data to an external device or system. The data can originate from IT servers or a computer system. The process can either be manual (copy-pasting) or automatic (through malware). Back in 2015, the security organization, McAfee, reported that the majority of the data exfiltration cases (Around 60%) were carried out through direct electronic means. The remaining 40% happened via physical media, for example, stealing a laptop or using a USB drive to download data. Interestingly, a significant portion of that 40% involved mobile phones. The data categories which were most exfiltrated were personal health information, personally identifiable information, financial data and intellectual property. Different kinds of tunneling protocols, file transfers, web protocols or email transfers are used in the electronic exfiltration of data. We know that the file transfer protocol is a standard network protocol meant to help us transfer files. It can also come in handy in data exfiltration campaigns.

Peripheral devices on the targets and other components such as microphones and webcams can be rigged to enable the monitoring of the target's activities. To stay anonymous, the hacker can use the Tor network or make use of HTTP file transfers. To prevent hackers from exfiltrating your data and staying safe from Advanced Persistent Threats, early detection is what will make the difference. It is important that organizations

possess a working threat intelligence mechanism that will aid in the identification of suspicious activities relating to data exfiltration. Linking the local threat intelligence system to the global threat intelligence network will help in keeping abreast of the latest trends in the security realm. Let me list some notable indicators of data exfiltration. These can be used as a platform to launch a comprehensive investigation. They are:

- Port activities that are not approved/sanctioned.
- Multiple email transmissions to non-corporate domains
- Excessive email sending by hosts
- Above normal DNS queries
- Web upload activity by the users. The uploads will normally be directed to non-corporate sites.

As I conclude this sub-topic, you have learned that for an attacker to obtain meaningful information, they will have to linger around their targets for some time. That implies that “Maintaining Access” is a key cycle of the hacking process which you will be required to master. This is easier said than done. Kali Linux comes with plenty of tools that can help you maintain access to a targeted system. Maintaining access is like getting into somebody else’s house without their permission. You will quickly realize that getting inside the house is just one part. Maintaining your presence without being detected is another. It may be even more difficult than the former task.

Clearing Tracks

In this step, we will be learning about how hackers cover their tracks with the objective of erasing any digital signs they may have left behind. It is obvious that this as an unethical activity. Simply put, it is concerned with the deletion of logs of the activities which took place during the hacking process. I am going to be very detailed in the covering of this sub-topic since it is of immense importance to the readers who seek to be professional hackers. There is one more process after clearing tracks, that is report writing, which is mostly paperwork. To know if a system has been targeted, we can carefully examine digital signs left behind by an intruder. It is in a hacker's interest to clear any traces of such activity that can lead to them. You may have noticed that in the previous phases, a penetration tester or hacker successfully avoided detection by intrusion detection systems and firewalls. In this phase, however, the objective is to conceal any hints that are likely to disclose the nature of the hacker's deeds.

The key components of covering/clearing tracks are:

1) Anti-Incident Response – these are measures that are meant to prevent real-time detection and,

2) Anti-Forensics – these are measures aimed at thwarting the collection of digital evidence during a possible post factum inquiry.

Anti-Incident Response

The main objective of Anti-Incident Response is to disrupt, confuse and out-maneuver the incident response team at work in the company, which was targeted. Additionally, activities falling under this category make it possible for a hacker/penetration tester to obtain a long-term foothold within their target even after they have been detected. Crucial tasks that can be carried out under anti-incident response include:

- Deployment of backdoors secretly
- Configuration of infrastructure to allow for agility in lateral movement
- Constantly updating the number of infected hosts. Also, their numbers should not be too large.
- Using a wide variety of malware on the network.
- Preventing investigators or responders from keeping up with what is going on by way of picking up the pace yourself.
- A perfect cover for internal hop-points can be provided by busy servers
- You can also use busy file servers as avenues for data staging.
- Using a VPN for communication in some cases may circumvent some measures put in place for network monitoring.
- Camouflaging the origin of malware transmission

The actions are undertaken in the prevention of immediate detection of an ongoing, or a continuous cyberattack is what matters when it comes to the working of an anti-incident response. The deliberate measures undertaken by hackers or penetration testers to destroy any evidence present and lead to a digital investigation to die out during the initial stages, anti-forensics, on the other hand, is designed to handicap the investigators' ability in

obtaining adequate digital evidence that will be submitted before a court of law during later stages. This, therefore, implies that activities under anti-incident response are urgent since a large portion of the action occurs on a live, running system in real-time. The countermeasures that the incident responders are likely to take are presumably much more time-constrained as compared to those by investigators in a potential digital investigation in the future.

Anti-Forensics

Before we start devouring this topic, let us first understand what forensics is. We define computer forensics as a discipline whose main objective is to enable the acquisition, preservation, analysis and presentation of digital evidence in a court of law by forensic experts. We define anti-forensics as a discipline that encompasses all the existing means and tools for purposes of deleting, modifying, or hiding digital evidence. The main objective of anti-forensics is the destruction, erasure, or manipulation of digital evidence. Anti-forensics has also been described by some as the "Attempts made to negatively compromise the quality, amount, and the existence of evidence from a crime scene or to complicate the examination and analysis of evidence so that it is impossible or difficult to conduct." One can tell from the name that this is involved with the techniques or actions that are supposed to create obstructions to an eventual digital investigation and to reduce both the quantity and quality of digital evidence. Cyber terrorists, hackers, counterfeiters, online pedophiles and other cybercriminals are among the typical users of anti-forensic techniques and tools. It is obvious that their intentions are to erase any existing traces capable of incriminating them.

Deleting Evidence

There are those of us who are so paranoid to the extent that they have invested resources on privacy protection tools and commercial disk cleaners solely to wipe data they do not wish others to lay their eyes on. It is believed that these tools can permanently delete everything from the hard disk. The specific information that can be deleted include:

- Web browsers history and cache
- Instant messengers chat logs including Skype and others
- Giving users a “secure delete” option with which they can wipe files
- Carry out the cleaning of these: registry items, thumbnails, jumplists, Skype chatsync and so on.

A forensic expert can use specific forensic tools to outsmart many of these clean-up programs. For example, pictures of interest to a forensic expert can be recovered. This is because even with the erasure of the original image, Windows Thumbnails will still have a smaller version of this picture. Even with the removal of the thumbnail, forensic can restore it by doing what we call file carving. Jumplists can also give information pertaining to pictures, applications, documents and numerous other types of files that the user has interacted with. The jumplists are normally created even for externally accessed files.

They will stay intact, regardless of whether there has been an erasure of the original file or that the external device has been removed. These lists will typically have a MAC address, the name, the path to the file being accessed, the application used to view the file, the computer name, alongside the time

and date that the item was accessed. This implies that jumplists can be used as an excellent proof of access. Deleting Skype history manually will not clean internal data stored in the "chatsync" folder. The folder's content can be used to unearth bits of user conversations. Despite the methods imperfectness (Deleting), when it is done properly, it can dispose of evidence irreversibly, leading the forensics experts to come out empty-handed.

Hiding, Moving, Renaming or Altering Files

This may sound naïve even though some of the wrongdoers can use this method to evade detection. The method used to cover tracks here can include renaming files, moving files containing conversation histories or changing file extensions. This, my friends, is not an easy task. There exist programs which can be used to break large files into small partitions. These partitions can be concealed at the end of other files. Using specialized programs, a hacker can use the unused file space, which is known as slack space, for hiding crucial information from plain sight. Additionally, a hacker can conceal a file inside another (You may have heard of stenography). This method works fine with executable files.

Timestamping

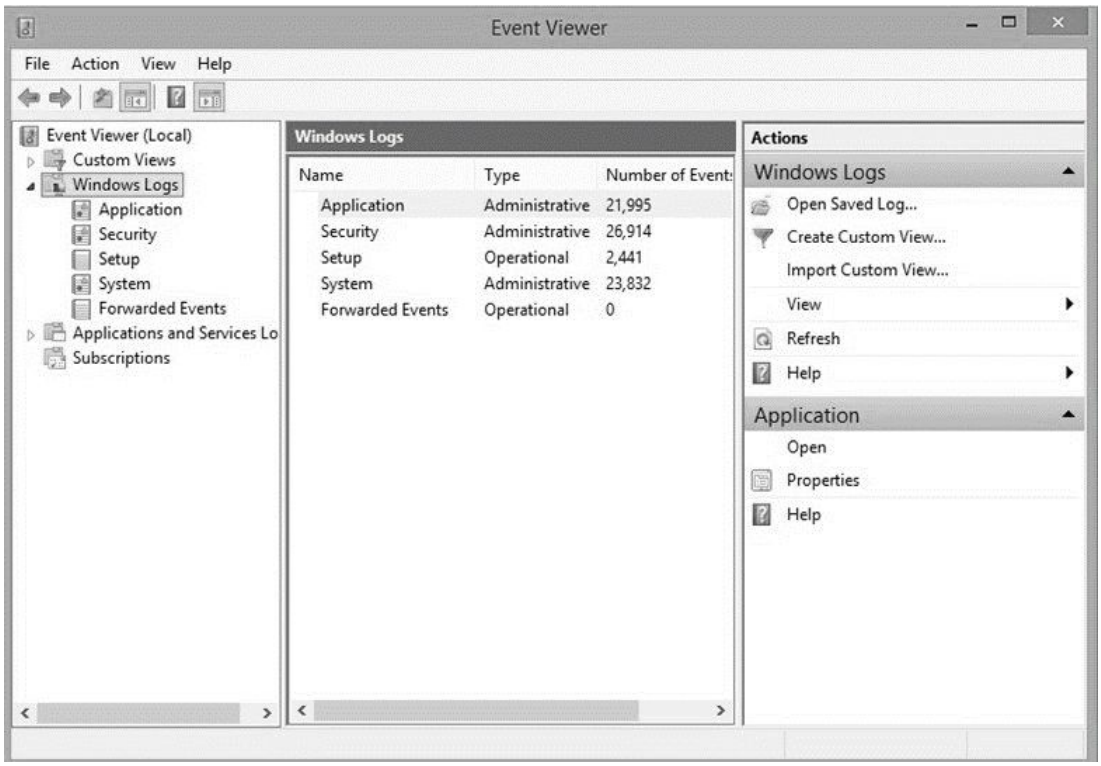
Many a time, the investigators do not normally examine all the files in a computer system. In most cases, they sort the information chronologically so that they can prioritize their search for potentially relevant information. They will want to view the information just at the time an attack occurred in cases where it is known. Criminals will typically attempt to counter this approach through the modification of the metadata belonging to the files

they require. Usually, they alter the times and the dates when each file was last accessed, last modified and when it was created. This anti-forensic technique is known as time stamping. Once the modification or transformation of a file has been done, the computer or device will think that the file is a different one. For instance, renaming an mp4 file to make it look like a .gif file.

Despite this, forensic investigators will normally depend on their experience and skills to find moved or renamed files. Also, we have methods for information forensics that can assess hard drives for suspicious discrepancies automatically. An example of such a method is data carving. This is a method that is used for carrying out a comprehensive and sequential scan of media. Data carving is effective in the sense that it can directly read low-level data from the media. It does not depend on the manner in which the file locations and names appear on the file system. For instance, an mp3 file is identified based on the contained actual data stream that is inherent to mp3 files and not based on the file's name.
Finally, encryption is a wonderful security measure a hacker can use. As far as digital forensics is concerned, encryption is a nightmare. Utilizing a strong encryption algorithm can result in the data being unreadable and will, therefore, be useless to the investigators.

Log Tampering

In computers running Windows, log files are typically kept in the event viewer. You can easily find it using the "Search" bar. The logs are stored in the/var/log directory in most Linux/UNIX operating systems.



System administrators can view any malicious activities that have occurred in their systems simply by examining the log files. We have two types of log files, the application generated and the system-generated log files. In log manipulation, a hacker normally has two options. One way is to completely delete the logs and the other way is to modify the contents of the log files. Here, a hacker can also replace the system binaries with malware such as Trojans to make sure that any evidence of cyber intrusion will not be detected. Deleting log files is not normally a good idea as it will create a gap in the logs files and this will raise suspicion. The log files can be used in the detection of malicious activities. They can be used as a warning system on the health and the actual state of a system. Any discrepancies in the logs will likely draw unwanted attention. A wise

attacker will likely carry out his attacks when the probability of viewing the log data is minimal say on weekends or during nighttime. An attacker will need to have root privileges to tamper with the information on log files. After escalating their privilege, a hacker can modify the log data associated with their activities within the log file itself. Any scrutiny by a system administrator will, therefore, not display any unusual activity. Prudent system administrators normally set up their system in a way that they will send all the log files to a remote server.

In summary

One precondition for success is being stealthy. Therefore, preventing detection during the hacking process is not enough. The process should continue even after the actual attack has been carried out. Any missteps will likely set off the radar detection and the forensics team will be quickly brought in to identify the attacker. This implies that the final step of covering tracks is of immense significance and should not be underestimated. If you wish to break into sophisticated systems, maintaining a low profile is a key skill that you will be required to have. We can say that covering tracks is a fail-safe technique that hackers employ to keep them out of trouble. The trouble can be immediate or after some time, say during an investigation.

Chapter 4: Wireless Network Hacking

Wireless Hacking

There are many advantages to using wireless networking. However, this kind of technology comes with a host of threats and vulnerabilities that hackers can take advantage of. Since information is sent over the air via radio frequencies, it is easier for hackers to intercept it compared to wired connections. This is more so when the information being sent is not encrypted or the encryption algorithm is weak.

Wireless networks consist of for basic elements:

- A wireless access point that connects to the network
- Data being transmitted via radio frequencies
- The Client device used, such as a laptop, tablet, etc.
- The users

Every one of these elements can be targeted by a hacker to compromise at least one of the three major objectives of a secure network: availability, integrity and confidentiality.

Wireless Network attacks

1. Accidental association

It is possible for a wireless network to be hacked accidentally. In some cases, one wireless network overlaps with another, thus enabling any user to jump into another unintended network accidentally. This may seem benign, but a malicious hacker can take advantage of this and gain access to information that should not have been exposed in such a manner. If the overlapping networks belong to organizations, then the link can be used to steal proprietary data.

2. Malicious Association

This occurs when malicious hackers gain access to a private network using their own device rather than through the legitimate access point (AP). A hacker can create a "soft AP," which can be a laptop with software that makes its wireless network card appear to be a genuine access point. This allows the hacker to steal passwords, attack computers or send users Trojan horse programs. A hacker can effectively have full control of every computer that joins the fake network.

3. Ad-hoc Networks

These are networks between two wireless computers with no access point separating them. Such networks can be attacked quite easily since they rarely have adequate protection.

4. Non-traditional networks

These include Bluetooth devices, wireless printers, handheld PDAs and barcode readers. These kinds of networks are rarely secured by IT personnel since all the focus is usually on laptops or access points. This makes them fair game for malicious hackers.

5. MAC Spoofing

This is a form of identity theft where a hacker monitors network traffic to identify which computer has network privileges. The aim is to steal the MAC (Media Access Control) address of that computer within the network. Many wireless systems have a MAC filter that allows only specific computers with specific MAC addresses to access and use the network. A hacker may get software that is able to "sniff" the network to find these authorized computers and their IDs and then employ other software that allows the hacker's computer to use these stolen MAC addresses.

6. Man-in-the-middle Attacks

This occurs when a malicious hacker sets up their laptop as a soft access point and then lures other users to use it. The hacker then connects the soft access point to a genuine access point using a different wireless card, thus forcing users to go through the fake AP to reach the real one. This enables the hacker to sniff out whatever information they want from the traffic. This type of attack has been made easier by software such as AirJack and LANjack. Wireless Hotspots are a great place to launch this kind of attack since there is hardly any meaningful security on such networks.

7. Denial of Service Attacks

This is where a hacker continuously sends numerous requests, commands and messages to a specific access point until the network crashes or just to prevent genuine users from getting onto the network.

8. Network Injection Attack

A malicious hacker injects counterfeit networking re-configuration commands into an access point that does not filter traffic. These fake commands bring down the entire network or switches, routers and hubs, forcing a reboot or reprogramming of every networking device.

Wireless Network Authentication

Wireless networks are designed to be accessible to anyone who has a wireless-enabled device. For this reason, most networks are protected using passwords. There are two common authentication techniques used: WEP and WPA.

WEP

This stands for Wired Equivalent Privacy and was developed to provide users with the same level of privacy as wired networks. It adheres to IEEE 802.11 WLAN standards. WEP encrypts data that is being sent over a network to prevent eavesdropping.

WEP vulnerabilities

There are significant flaws in the design of this type of authentication technique:

1. It uses Cyclic Redundancy Check 32 to verify the integrity of packets. The problem with CRC32 is that a hacker only needs to capture two packets to crack into the network. They can also modify the checksum and encrypted stream to force the system to accept the packet.

2. It uses an RC4 encryption algorithm to make stream ciphers composed of a secret key and an Initial Value (IV). The IV length is fixed at 24 bits, but the secret key can be 40 to 104 bits in length. If a secret key of a lower length is used, the network becomes easier to hack.

3. Since it is a password-based authentication technique, a hacker can successfully deploy a dictionary attack.

4. It does not have a central key management system, thus making it very difficult to change keys in big networks.

Due to the numerous security flaws, WEP has fallen out of favor and replaced by WPA.

How to crack WEP networks

Exploiting the numerous security vulnerabilities on a WEP network is possible either through passive attacks or active cracking. If a passive attack is launched, the network traffic is not affected until WEP authentication has been successfully cracked. This makes it harder to detect. Active cracking tends to increase the load on the network, thus making it easier to detect, though it is also more effective.

The tools that can be used for cracking WEP include:

Aircrack — This is also a network sniffer and can be downloaded from www.aircrack-ng.org/

Kismet — This multi-purpose tool can sniff network packets, detect invisible and visible networks and even identify intrusions. It can be downloaded from www.kismetwireless.net/

WEPCrack — This open-source tool can crack secret keys and can be downloaded at www.wepcrack.sourceforge.net/

WebDecrypt — It cracks WEP keys using a dictionary attack and generates its own keys. Get it at www.wepdecrypt.sourceforge.net/

WPA

WPA is an abbreviation for Wi-Fi Protected Access. It was primarily developed to mitigate the weaknesses of WEP. WPA uses greater IV than WEP, 48 bits to be precise. Packets are encrypted using temporal keys.

WPA vulnerabilities

1. Hackers can easily overcome it using denial of service attacks.
2. Its keys rely on passphrases and if weak passphrases are used, a dictionary attack can be successfully launched.

How to crack WPA networks

Since WPA uses passphrases to authenticate user logins, a well-coordinated dictionary attack makes it vulnerable, especially if short passphrases are used. The tools for cracking WPA include:

Cain and Abel — It is used to decode files that have been sniffed by other programs like Wireshark.

CowPatty — This is a brute force attack tool that cracks pre-shared keys. Download from wirlessdefenc.org/Contents/coWPAttyMain.htm

How to crack network WPA and WEP keys

You are going to need the right software, hardware and patience in order to crack the keys to a wireless network. However, successfully doing so is dependent on the activity levels of users within the network you have targeted.

Backtrack is a great security operating system that is based on Linux. It contains many well-known tools that are very effective for collecting data, evaluating weaknesses and exploiting networks. Some of these tools include Metasploit, Ophcrack, Wireshark, Nmap and Aircrack-ng.

Cracking network authentication keys requires the following:

- Wireless network adapter able to inject packets.
- Backtrack OS, downloadable from backtrack-linux.org/downloads/
- Proximity to the network radius.
- Adequate knowledge of Linux OS and how to use the scripts in Aircrack.
- Patience, as there are factors that you may not be able to control.

Remember, the greater the number of people actively accessing the network, the faster this will work.

How to perform MAC spoofing

To carry out MAC spoofing, you will have to bypass the MAC filtering that the target network is using. MAC filtering is commonly used to lockout MAC addresses that have not been authorized to connect to a wireless network. This is usually an effective way to prevent people who may somehow acquire the password from connecting to the network. However,

MAC filtering is not an effective security measure when it comes to locking out hackers.
The steps below will show you exactly how to go about spoofing the MAC address of a client who is authorized to connect to the network. The Wi-Fi adapter should be in monitoring mode. Airodump-ng on Kali Linux will be used to recover the MAC address. After this, the Macchanger program will be used to do the spoofing, bypass the filter and connect to the network.

Instructions:
1. Make sure your Wi-Fi adapter is in monitoring mode. To find the wireless network that is being targeted as well as any clients connected to it, enter this command:

Airodump-ng—c [channel]-bssid [target router MAC Addres]-l wlan0mon

A window will open up, displaying a list of clients who are connected to the network. Their whitelisted MAC addresses will also be shown. These are the addresses you need to spoof to enter the network.
2. Pick one of the whitelisted MAC addresses from the list to use to spoof your own address. Before you can perform the spoofing, you must take down the monitoring interface. Enter the command:

Airmon-ng stop wlan0mon

3. The next step is to take down the wireless interface of the MAC address you intend to spoof. Enter the command:

Ifconfig wlan0 down

4. Then you use the Mcchanger software to change the address. Enter the command:

Macchanger —m [New MAC Address] wlan0

5. Remember, you had taken down the wireless interface in step 3. Now it is time to bring it back up. Use the command:

Ifconfig wlan0 up

Now that the MAC address of your wireless adapter has been changed to that of an authorized user, test and see if the network will authenticate your login. You should be able to connect to the wireless network.

Transmissions

Hacking of wireless networks poses three main threats: Disruption, Alteration and Interception. To prevent malicious hackers from eavesdropping on wireless transmission, you can use:

Signal-hiding methods — Before a malicious hacker can intercept wireless transmissions, they first have to locate the wireless access point. An organization can make this more difficult by switching off the SSID (service set identifier) being broadcast by the access point, assigning a cryptic name to the SSID, lowering signal strength to provide just enough

requisite coverage or stationing access points away from exterior walls and windows. There are also more effective but expensive techniques, such as employing directional antennas to restrict the signal within a specific area or using TEMPEST (a technique to block the emission of wireless signals).

Stronger encryption of all wireless traffic — This is very important, especially for organizations that must protect the confidentiality of their information being broadcast wirelessly. This measure reduces the risks of a man-in-the-middle attack.

Stronger authentication procedures — This should apply to users as well as their devices. This minimizes man-in-the-middle attacks.

Countermeasures against Denial of Service Attacks

Malicious hackers may, at times, attempt to bring down the servers of an organization, but in some cases, a DOS attack may be unintentional. There are certain steps that can be taken to minimize the risks of this form of attack:

- Performing site surveys carefully to determine the location of signals emanating from other devices. This should be used as a guide in deciding where the access points should be located.

- Conducting regular audits of network performance and activity to determine areas with problems. If there are any offending devices, they should be removed. Measures should also be taken to enhance signal coverage and strength in problem areas.

Access Points

Wireless access points that are poorly configured are a major vulnerability and may allow malicious hackers unauthorized access to confidential information. To secure wireless access points, the following countermeasures must be taken:

- Eliminate all rogue access points — The best way to do this is to use 802. Ix to prevent any rogue devices from plugging into and connecting to the wireless network.

- Ensure all authentic access points are properly configured — Make sure that all default settings are changed since they are publicly available and hackers can easily exploit them.

- Authenticate every device using 802. Ix protocol — a strong authentication system will prevent unauthorized devices from setting up backdoors. This protocol ensures stringent authentication before assigning any device to an IP address.

Devices

There are two perspectives when it comes to assessing security threats against wireless devices: Theft/Loss and Compromise. Laptops and PDAs usually contain a lot of confidential and sensitive information and therefore must be protected from theft or loss. Wireless client devices can also be compromised when a malicious hacker gains access to stored data in the device. Hackers can also use the device to launch attacks on other systems and networks.

Networks

- Encryption — This is the best way to secure a wireless network. Most base stations, access points and wireless routers come with inbuilt encryption mechanisms that enable scrambling of network communications. Always make sure that the router you buy comes with an encryption feature. Most manufacturers turn this feature off, so ensure that you manually turn it on before you start using your router.

- Anti-spyware, anti-virus and firewalls — Make sure that your wireless network is protected in the same way as a wired connection. Keep all your software updated and always check whether your firewall is switched on.

- Switch off your router's identifier broadcasting - This is the mechanism that a wireless router uses for broadcasting its presence in an area. However, there is no need to announce the presence of a network if the users know that it is already there. Malicious hackers tend to search for the identifier broadcast to zero in on potential targets.

- Change default identifier — Every router has a default ID given to it by its manufacturer. You may have switched off the identifier broadcaster, but hackers can still attack the network if they find out the default ID, which is publicly accessible. Change the identifier and do not forget to configure the new ID into your computer.

- Change the default password — Every router is assigned a default password by the manufacturer. This is for purposes of configuring the

device initially. These default passwords are easy to find, so make sure that you change your router password to something that will be very difficult to crack. Also, try to make your password as long as possible.

- Specify the devices authorized to connect to the network — Configure your router to only allow specific Mac addresses to connect to the network. However, do not rely on this technique alone, as Mac spoofing is still possible.

- Shut the network down when unused — Whenever a wireless network is not being used, make sure that it is switched off. This will limit the window of opportunity that hackers can use to penetrate the network.

- Be vigilant in W-Fi hotspots — Most people love to use the free Wi-Fi at airports, cafes, hotels and other public places. These wireless networks are rarely secured, so do not assume that they are.

The Users

There is no greater way to secure a wireless network than educating and training all users. Users are not just people who connect to the network but IT personnel and administrators as well. It is very important to teach people how to behave in a way that will maintain the security of the wireless network. This user training and education must be a periodic endeavor.

Let us face it. It is not possible to completely eliminate every risk that a wireless network comes with. Eventually, a hacker will get through. However, there are actions that can be taken to maintain a reasonable level

of general security. This is possible using systematic risk evaluation and management techniques. Every component of a wireless network must be considered when establishing countermeasures against malicious hackers.

Chapter 5: Uses and Applications of Kali Linux

The uses of Kali Linux are wide-ranging. Below, I have outlined and discussed some of them. Feel free to download the documentation from the links provided in chapter 2. Now let us get down to the serious stuff.

Penetration testing

This is a mechanism that is utilized by organizations to ascertain the robustness of their security infrastructure. Here, security professionals will play the role of the attackers, whereby they will attempt to discover flaws and vulnerabilities in a system before the malicious fellows do. One key objective is the identification and reporting of vulnerabilities to companies and organizations. As organizations become increasingly security conscious and the cost of security breaches rises exponentially, many large organizations are beginning to contract out security services. One of these critical security services is penetration testing. A
penetration test is essentially a legal, commissioned hack to demonstrate the vulnerability of a firm's network and systems. Generally, organizations conduct a vulnerability assessment first to find potential weaknesses in their network, operating systems and services. I emphasize potential, as this vulnerability scan includes a significant number of false positives (things identified as vulnerabilities that are, in reality, not vulnerabilities). It is the role of the penetration tester to attempt to hack, or penetrate, these

vulnerabilities. Only then can the organization know whether the weakness is real and decide to invest time and money to close the vulnerability.

Espionage and military

Cyber espionage can be said to be the practice of accessing information and secrets without the knowledge and permission of the entities being targeted. They can be ordinary individuals, rivals, competitors, groups, governments or even enemies. The objectives here are broad. They can be political, economic, personal or even military-related. The techniques used, too, are diverse. Hackers can use malicious software, cracking techniques, proxy servers, among others, to attain their stated objectives. Espionage can be carried out online by professionals from their computer desks or it can be done by infiltration using trained moles and conventional spies. In some circumstances, it can be carried by amateurish hackers with malicious intent and software programmers. It is common knowledge that every nation on earth carries out some form of cyber espionage or even cyber warfare, albeit covertly. Gathering intelligence on military activities of other countries has been made more cost-effective by hacking. Thus, a hacker has their place cut out in the defense systems of any nation.

Forensics:

For years, the popularity of Forensic Linux Live Boot environments has become well known. There are so many forensic tools that are Linux based on this distribution. Using Kali, forensic experts can do all that pertains to their tradecraft starting from the initial triage, data imaging all the way to case management and full analysis.

Reverse Engineering:
Recently, reverse engineering has become an indispensable skill in various sectors, including law enforcement. Reverse Engineering is a primary method that is used in the identification of vulnerabilities and the development of exploits. That is on the offensive side of it. Defensively speaking, reverse engineering can be utilized in the analysis of malware that has been used to target a given system. Here, the objective will be to establish the capabilities of a given piece of tradecraft.

Wireless Attacks:
Kali supports a wide range of wireless hacking tools. What makes wireless networks a commonly attacked vector is their pervasive nature. Kali Linux also supports multiple wireless cards and is a hacker's favorite choice for conducting attacks against different types of wireless networks.

Password Attacks:
Kali Linux can be used for conducting password attacks where a user encounters an authentication system. The OS comes with numerous useful tools and utilities for this purpose. We have both offline and online password attack tools that a Kali Linux user can use to deal with hashing and encryption systems.

Database Assessment:
Kali Linux is capable of database attacks such as SQL injection and attacking credentials. All this is made possible by the tools present in Kali's vast repositories that can be used for testing attack vectors ranging from data extraction and analysis to SQL injection.

Sniffing and Spoofing:
Again, Kali Linux has plenty of tools an aspiring hacker or a professional one can use to get access to data as it is being transmitted over the network. You can use spoofing tools to impersonate a networks' legitimate user and then use the sniffing tools if you wish to capture and analyze data you have just captured. These tools are a lethal combination when used together.

Stress Testing
To check whether your system is stable, you carry out a stress test on it. In this scenario, you will use the numerous tools provided by Kali Linux to generate more than normal traffic. This way you will be able to know the limits of your system. The tools for stress testing can either be proprietary or open-source. As an expert, it is essential that you know all the tools that are used for testing a system's availability.

Hardware Hacking
Another application of Kali Linux is in hardware hacking. Kali Linux comes with the following tools that can be used to accomplish this task.

- **android-sdk** - The Android SDK provides you the API libraries and developer tools necessary to build, test and debug apps for Android.

- **apktool** - It is a tool for reverse engineering 3rd party, closed, binary Android apps. It can decode resources to the nearly original form and rebuild them after making some modifications; it makes possible to

debug smali code step by step. Also, it makes working with the app easier because of project-like files structure and automation of some repetitive tasks like building apk, etc.

- **Arduino** - This is an electronics prototyping platform that is open-source. It is based on easy-to-use, flexible software and hardware.

- **Sakis3G** - Sakis3G is a tweaked shell script that is supposed to work out-of-the-box for establishing a 3G connection with any combination of modem or operator. It automatically setups your USB or Bluetooth™ modem and may even detect operator settings. You should try it when anything else fails.

- **Smali** - smali/baksmali is an assembler/disassembler for the dex format used by dalvik, Android's Java VM implementation. The syntax is loosely based on Jasmin's/dedexer's syntax and supports the full functionality of the dex format (annotations, debug info, line info, etc.)

Chapter 6: Introduction to Cybersecurity

Introduction

We define cybersecurity as being the protection of computer systems, computer networks, and their associated programs from attacks that are of a digital form. Typically, cyberattacks are carried out with the intent of gaining access, modification or even destruction of information that is sensitive. They also attempt to extorting money from victims and are meant to interrupt the normal processes of a business.

Confidentiality, Integrity and Availability

The three are famously referred to as the CIA triad. We can describe it as a model whose purpose is to guide information security policies within any given organization. To prevent confusing the triad with the American Central Intelligence Agency, we sometimes refer to it as the AIC triad. The three elements are the most critical components of security. In our case, we can say that availability is defined as a guarantee of access that is reliable to information by people with authorization, confidentiality is said to be a set of protocols that are used to limiting access to information and integrity is the undertaking given to show that the information at hand is both accurate and trustworthy.

Confidentiality:

This is a rough equivalent of privacy. While ensuring that the right people can have access to crucial information, it is also prudent that vigorous measures are undertaken to make sure that there is confidentiality. There should be restricted access to the data in question by those who are authorized to view it. Out there, it is not uncommon to categorized data based on the type and amount of damage that can result from it falling into unauthorized persons. Stringent measures can more or less be implemented depending on these categories. Guarding the confidentiality of data sometimes requires specialized training for authorized to view/use persons. It would generally involve security risks that could harm that information. It can, without a doubt, help people with the proper authorization to get to know the various risk factors and equip them with countermeasures. Additional aspects of the training may comprise best practices in password-related issues alongside social engineering mechanisms.

This will help them avoid breaching rules governing data-handling with potentially disastrous results in as much as they may have intentions we can describe as being noble. For example, using a routing number or an account number is an effective measure that can be used to ensure confidentiality. We can also employ the use of data encryption to make sure that there is confidentiality. Passwords and user IDs are part of a standard procedure that is becoming a common phenomenon, two-factor authentication. There are different options. They include security tokens (soft tokens or key fobs) and biometric verification.

Furthermore, it is incumbent upon the users to take precautions in ensuring that locations where their information appears and the number of times required to send it to complete a transaction is at a minimal. In cases where we have critical data, extra measures may be necessary. Such actions can involve storing the information on disconnected storage devices on air-gapped computers or it can even be stored in the form of hard copies only.

Integrity:

This component of the triad comprises ensuring the trustworthiness, consistency, and accuracy of data throughout its complete life cycle. It is of immense importance that data that is in transit is not altered. Solid steps need to be taken to make sure that no modification on the data by unauthorized people happens. For instance, in cases where we have a confidentiality breach. Here, the countermeasures can involve user access controls and file permissions. To prevent accidental deletion or erroneous changes by authorized users, we can employ the use of version control. In place, there also need to exist mechanisms to help in the detection of data changes, which may result from non-human events, including a server crash or an electromagnetic pulse. We can include checksums and cryptographic checksums to help with the integrity verification of data. Lastly, it may be necessary to have some form of redundancies and backups that will help in the restoration back to its former state.

Availability:

The rigorous maintenance of all the hardware ensures that there will always be availability fo the services rendered by this hardware. Failing equipment should be promptly and adequately repaired to keep in order a properly functioning operating system environment that is devoid of any software

conflicts. One aspect of maintenance that should also be carried out is updating all the necessary system components. It will also be to provide ample bandwidth for communications and to ensure a minimal occurrence of bottlenecks. Mitigation of hardware failures and their repercussions can be done using high-availability clusters, redundancy, RAID and even failovers.

For the worst-case scenarios that occur, disaster recovery that is both adaptive and fast is essential. For this to be possible, the disaster recovery plan laid down has to be comprehensive. Prevention of data loss or connection interruptions needs to also account for unpredictable events. Examples include fire and natural disasters. Copies of back up data can be securely stored at a location that is geographically-isolated to prevent loss of data resulting from such occurrences. Such sites also need to be water and fire-resistant. To guard against issues such as downtime and inaccessibility of data due to denial-of-service attacks and network intrusions, we can employ the use of extra security equipment, for instance, proxy servers, firewalls and software.

Issues arising from the CIA:

The CIA paradigm faces immense challenges where big data is involved. This is primarily because of the sheer volume needing to be kept safe, the variety of formats of the data, and, finally, the multiplicity of the originating sources. Disaster recovery plans and duplicate sets of data all make the already high cost even higher. Additionally, oversight is often lacking since the main objective of big data is for analytics purposes, i.e., gathering data and using it to make some kind of useful interpretation. We all know this fellow, Edward Snowden, who brought this issue to light. Security agencies

carry out the collection of enormous volumes of peoples' private data throughout the world. To safeguard individual information from exposure in the IoT environment, we have special considerations known as the Internet of Things privacy. This means that almost any logical or physical entity can be assigned a unique identifier to enable autonomous communications over a network, including the Internet.

The transmitted data from a particular endpoint may not, on its own, necessarily result in any privacy issues. The catch is, however, when the fragmented data from multiple endpoints is accessed, gathered and analyzed, sensitive information can be obtained. Securing the Internet of Things is itself a formidable challenge since it comprises numerous Internet-enabled devices besides computers. Such devices are, in most cases, often set up with default passwords that are weak or in some cases, the devices are unpatched. Unless IoT is protected adequately, there is a likelihood that it may be used as a separate vector of attack or be made a part of a thingbot. Recently, it has been demonstrated by researchers that it is possible to compromise a network just by using a Wi-Fi-enabled light bulb. It is essential for us that we consider the security of the numerous network-capable products that are under development.

Encryption

We define encryption as a mechanism through which plaintext or other data type are changed from their currently readable form to an encoded way. It is only an entity having access to a decryption key that can decode the data. This is an important measure that usually is used to provide end-to-end data

security across networks. Encryption, as a proactive security measure, is commonly used all over the internet for purposes of protecting crucial information belonging to users, which is being exchanged between servers and browsers. That can include private information such as payment information, passwords and other personal information. Individuals, together with organizations, may also opt to use encryption to ensure the safety of sensitive data that is stored on mobile devices, servers and computers.

How encryption works

Plaintext data, also known as unencrypted data, is encrypted through the use of an encryption algorithm plus an encryption key. The result of this is a ciphertext that can be seen only in its original form if decrypted with the correct key. On the other hand, decryption is the reverse of encryption. The steps used in encryption are followed in a reverse fashion. In the modern age, we have two commonly used encryption algorithms. They are symmetric and asymmetric encryptions.

When it comes to the symmetric encryption mechanism, a single key is utilized for encryption. The Advanced Encryption Standard (AES) is one of the most used symmetric-key ciphers. It was designed primarily to protect classified information for governments. This mechanism is faster in comparison to asymmetric encryption. The sender must, however, share the encryption key with the recipient. The keys need to be managed in a secure fashion. This uses an asymmetric algorithm in most cases.

On the other hand, we have asymmetric cryptography. We can also refer to it as public-key cryptography. Here, two different keys are used. They are,

however, mathematically linked. The keys are as follows; one key is public and the other one private. The public key many times can be shared with anyone. The private key has to be kept secret. In asymmetric cryptography, the commonly used encryption algorithm is the RSA. The reason is to some extent that the two keys can encrypt a message, which is to imply the key that is opposite to the one used for the encryption is used to decrypt it. This feature offers a way of ensuring that we not only have confidentiality but also authenticity, non-reputability and integrity of electronic communications and data.

Benefits of Encryption

Confidentiality of digital data, which is stored on computer systems or that which is sent through the internet or any other computer network, is protected by using encryption. Organizations such as Payment Card Industry Data Security Standard (PCI DSS) require that sensitive data be encrypted to keep unauthorized entities from accessing the data. We also have some standards requiring or recommending data encryption. Nowadays, modern encryption algorithms serve an integral role in making sure that the security of communications and IT systems possess not only confidentiality but also the under listed key elements of security:

- Authentication: the origin of a given message should be able to be verified.
- Integrity: This has got to do with keeping the message intact. That is, the contents of messages have not been altered or deleted from the time it was sent.
- Nonrepudiation: Here, non-repudiation means that a particular sender cannot dispute that they send the message.

Backup and Redundancy

Usually, we use backup where copies of data are created in anticipation of a catastrophic loss. On the other hand, redundancy is a lot more than just data storage. Redundancy aims to provide a continuity of service regardless of what will happen. Data redundancy ensures that the storage of data is done at multiple and heterogeneous locations. We also have what we call network redundancy whereby a given network is configured in such a way that it has numerous alternative systems. The alternative systems serve to ensure continuity of service regardless of what happens.

Data Redundancy

For any organization, it is essential first that regular services are restored as soon as possible after there has been a security breach. Data should be able to be reconstructed as quickly as possible. To this end, businesses have come up with various ways to make sure there is data redundancy. It is common knowledge that these methods come with their own merits in terms of cost-effectiveness, speed and management. The most common way is using off-site tape backups. In this method, magnetic tapes are used to store a complete bit-for-bit copy of a storage volume. The tapes can be transferred to an off-site storage facility where they can be easily retrieved whenever there is a catastrophic failure. Besides, we can use Cloud Backup to safeguard data against losses.

Network Redundancy

Most of the infrastructure we use for our networks are unbelievably fragile. For instance, when a router burns out due to one reason or another, the result is that there will be a prolonged period of network downtime. To mitigate against this, businesses make sure that networks they use have an adequate redundancy so that they can survive and provide services in cases of an emergency. Fundamentally, network redundancy means that no matter what type of failure occurs, a network will still be up and running. To be able to do this, we can have multiple network devices such as hubs, routers and switches configured to stand in for one of them that fails. We also have ISP redundancy, where a gateway in the network is joined to more than one separate ISP. Just like with the devices, one ISP will take over whenever there is a failure. In cases where a network is functioning correctly, we can use the ISPs to share the traffic resulting in reduced congestion of the network. This here is called load sharing.

Preventing a SPOFF

SPOFF is full for a single point of failure. We do not desire that one critical part of a system failure can render the entire system unusable. Any planning needs to mitigate this phenomenon. A single point of failure can be reduced or eliminated by way of redundancy. This will make sure that there is not a single component that can prevent the proper working of a system.

Chapter 7: Network Scanning and Management

Introduction

The ability to scan for and connect to other network devices from your system is crucial to becoming a successful hacker, and with wireless technologies like WiFi
and Bluetooth becoming the standard, finding and controlling WiFi and Bluetooth connections is vital. If someone can hack a wireless connection, they can gain entry to a device and access to confidential information. The first step, of course, is to learn how to find these devices. In this chapter, we are going to examine two of the most common wireless technologies in Linux: WiFi and Bluetooth.

Network Scanning

We say that it is the utilization of a computer network for purposes of collecting information about IT systems. We carry out scanning of networks primarily to help us do system maintenance or a security assessment. Hackers can also conduct a network scanning exercise before launching their attacks. The following are some of the reasons we scan networks:

- Identification of the present TCP and UDP network services, which may be actively being executed on the targets.
- To get to understand the systems for filtering that are in between the targeted hosts and the user.
- Discover the operating systems that are being used through the assessment of their IP responses.
- Analyze a particular host that is being targeted for its number predictability of the TCP sequence. This is to enable the TCP spoofing and attack sequence prediction.

Network scanning comprises of two key aspects: vulnerability scanning and network port scanning. The latter denotes a way of sending data packets through a network over to a systems' specific port numbers. The goal is to discover network services that are present in that particular system. It is an excellent way for troubleshooting issues that a given system has. That way, the problems can be dealt with so that the system is secure. For us to discover known vulnerabilities present in network systems, a method known as vulnerability scanning is used. Through it, we can identify weak spots both in the operating system and the application software. It is these weak points that are usually used to compromise computing systems.

Both vulnerability scanning and network port scanning can be said to be techniques that are used in information gathering. On the flip side, they can be a prelude to an attack when they are put to use by anonymous entities. Such entities usually have malicious intentions. The inverse mapping is another technique for network scanning. It is useful when it comes to collecting IP addresses that are not mapped to live hosts. By doing so, it will be aiding in the focussing attention on addresses that are worth

focussing on, that is, those that are feasible. There are three stages in which information gathering can be accomplished.

i. The footprinting stage
ii. The scanning stage
iii. The enumeration stage

This, therefore, implies that network scanning is among the crucial steps an attacker needs to be able to gather information.

Network scanning with ifconfig

The ifconfig command is one of the essential tools that can be used for examining and interacting with active network interfaces. You can use it to query your active network connections by simply entering ifconfig in the terminal.

Scanning Wireless Networks with iwconfig

If you have a wireless adapter, you can use the iwconfig command to gather crucial information for wireless hacking, such as the adapter's IP address, its MAC address, what mode it's in and more. The information you can glean from this command is particularly important when you're using wireless hacking tools like aircrackng.

Changing your network information

Being able to change your IP address and other network information is a useful skill because it will help you access other networks while appearing as a trusted device on those networks. For example, in a denial of service (DoS) attack, you can spoof your IP so that that the attack appears to come

from another source, thus helping you evade IP capture during forensic analysis. This is a relatively simple task in Linux and it's done with the ifconfig command.

Changing Your IP Address

To change your IP address, enter ifconfig, followed by the interface you want to reassign and the new IP address you want to be assigned to that interface. For example, to assign the IP address 192.168.181.115 to interface eth0, you would enter the following:

```
Kali >ifconfig eth0 192.168.181.115
kali >
```

When you do this correctly, Linux will go back to the command prompt and say nothing. This is a good thing! Then, when you again check your network connections with ifconfig, you should see that your IP address has changed to the new IP address you just assigned.

Changing Your Network Mask and Broadcast Address

You can also change your network mask (netmask) and broadcast address with the ifconfig command. For instance, if you want to assign that same eth0 interface with a netmask of 255.255.0.0 and a broadcast address of 192.168.1.255, you would enter the following:

```
Kali >ifconfig eth0 192.168.181.115 netmask 255.255.0.0 broadcast
192.168.1.255
kali >
```

Once again, if you've done everything correctly, Linux responds with a new command prompt. Now enter ifconfig again to verify that each of the parameters has been changed accordingly.

Spoofing Your MAC Address

You can also use ifconfig to change your MAC address. The MAC address is globally unique and is often used as a security measure to keep hackers out of networks —or to trace them. Changing your MAC address to spoof a different MAC address is almost trivial and neutralizes those security measures. Thus, it's an instrumental technique for bypassing network access controls. To spoof your MAC address, use the ifconfig command's down option to take down the interface (eth0 in this case). Then enter the ifconfig command followed by the interface name (hw for hardware, ether for Ethernet) and the new spoofed MAC address. Finally, bring the interface back up with the up option for the change to take place.

IP Addresses assignment

Linux has a Dynamic Host Configuration Protocol (DHCP) server that runs a daemon, a process that runs in the background, called dhcpd or the dhcp daemon. The DHCP server will carry out the assignment of IP addresses to all of the systems that are located on the subnet. It also keeps a log of which IP address is allocated to which machine at any one time. This makes it an excellent resource for forensic analysts to trace hackers after an attack. For

that reason, it's useful to understand how the DHCP server works. Usually, to connect to the internet from a LAN, you must have a DHCP-assigned IP.

Therefore, after setting a static IP address, you must return and get a new DHCP-assigned IP address. To do this, you can always reboot your system, but I will show you how to retrieve a new DHCP without having to shut your system down and restart it. To request an IP address from DHCP, all that is required is to call the DHCP server using dhclient, followed by an interface that you wish to assign the address. The different Linux distros use different DHCP clients. Kali, for instance, is based on Debian that uses dhclient.

Manipulating the Domain Name System (DNS)

Hackers can find a treasure trove of information on a target in its Domain Name
System. This is a key element of the internet and although it's designed to translate domain names to IP addresses, a hacker can use it to garner information on the target.

- **Examining DNS with dig**

DNS is the service that translates a domain name like google.com to the appropriate IP address. This way, your system knows how to get to it. Without DNS, it would mean that we would be required to remember the thousands of IP addresses that belong to the websites we visit frequently. Dig is one of the commands any aspiring hacker needs to know. It offers a way to gather DNS information about a target domain. The stored DNS

information can be a crucial piece of early reconnaissance to obtain before attacking. This information could include the IP address of the target's nameserver (the server that translates the target's name to an IP address), the target's email server and potentially any subdomains and IP addresses. You can also use the dig command to get information on email servers connected to a domain by adding the mx option (mx is short for mail exchange server). This information is critical for attacks on email systems.

- **Changing Your DNS Server**

In some cases, you may want to use another DNS server. To do so, you will edit a plaintext file named /etc/resolv.conf on the system. Open that file in a text editor. Then, on your command line, enter the precise name of your editor, followed by the location of the file and the filename.

Wi-Fi Networks

Firstly, let us look at WiFi. Before doing so, here is a small introduction to the various WiFi security protocols that usually are frequently used. The original, Wired Equivalent Privacy (WEP), was severely flawed and easily cracked. Its replacement, WiFi Protected Access (WPA), was a bit more secure. Finally, WPA2PSK, which is much more secure and uses a preshared key (PSK) that all users share, is now used by nearly all WiFi AP's (except enterprise WiFi).

Basic Wireless Commands

ifconfig

To perform a network interface configuration in Unix-based operating systems, one needs ifconfig. It is an administration utility that is found in the system. Ifconfig has utilities that are utilized in the configuration, querying and controlling of the parameters of the TCP/IP interface. As an interactive tool, ifconfig can be used to show settings of the network interface and analyze them.

In summary, ifconfig does the following:

- The command enables the viewing of settings of a network;
- Carrying out enabling of a network Interface and also disabling it;
- Network Interface IP address assigning ;
- Assigning network interfaces a netmask ;
- Allocating a Broadcast to Network Interface;
- Assigning an IP, Netmask and Broadcast to Network Interface;
- Changing MTU for a Network Interface;
- Enabling and disabling Promiscuous Mode;
- Addition and removal of New Alias to Network Interface;
- Changing the MAC address of Network Interface.

iwevent

This command displays Wireless Events received through the RTNetlink socket. Each line shows the specific Wireless Event, which describes what has happened on the specified wireless interface. This command doesn't take any arguments.

iwlist

This command can be used for scanning wireless networks available and also for displaying any other information about the wireless networks which are not displayed when the iwconfig command is used. Iwlist is utilized in the generation of wireless access points that are nearby together with their SSIDs and their MAC addresses.

iwspy

This command is used for monitoring nodes in a network. It can also be used for recording the link quality of the nodes.

ifrename

This command is used for renaming wireless network interfaces depending on multiple criteria that are static to allocate names consistently to each interface. The interface names usually are dynamic by default. This command helps users decide the name of the network interface.

iwgetid

This is used in the reporting of the NWID, ESSID or address of the access point of the wireless network presently being used. By default, iwgetid will display the devices' ESSID. Suppose that it is unavailable, it will output its NWID instead. The information reported is the same as the one shown by iwconfig. In comparison, it is easier to do integration in various scripts.

Detecting and Connecting to Bluetooth

In recent times, nearly all gadgets, systems and devices have inbuilt Bluetooth. The devices can be computers, iPods, smartphones, speakers, game controllers, keyboards, tablets, among others. The ability to break into Bluetooth networks can result in the compromising of the information on

the device, assuming a devices' control and acquisition of a platform to transmit privileges information from and to the device, among other things. We, therefore, need to understand how Bluetooth works if we are to exploit this technology. From this book, you will be able to acquire some basic knowledge that will come in handy during the scanning and connecting to Bluetooth devices in preparation for hacking them.

How Bluetooth Works

First, we can define Bluetooth as a wireless communication technology that enables devices to transmit voice or data wirelessly. This happens over a relatively short distance. This technology was meant to replace the ubiquitous cables that were being used to connect devices while still securing the communications across them. The process of joining two Bluetooth devices is known as pairing. Pretty much any two devices can pair if they are set to a discoverable mode. In the discoverable mode, a Bluetooth device will broadcast the following information about themselves:

- Technical information
- Name
- List of services
- Class

Upon pairing, two Bluetooth devices will exchange a link key. The devices will store the key to be used in the identification of the other device in future pairings. Every device has a unique identifier and usually a manufacturer-assigned name. These will be useful pieces of data when we want to identify and access a device.

Bluetooth Scanning and Reconnaissance

Linux has an implementation of the Bluetooth protocol stack called BlueZ that we are going to use to scan for Bluetooth signals. Most Linux distributions, including Kali Linux, have it as an inbuilt feature by default. BlueZ possesses utilities that can help us scan and manage Bluetooth capable devices. Examples of the utilities are outlined below:

- hciconfig: this is an equivalent of ifconfig in Linux, but made for Bluetooth capable devices.
- hcitool: this is a tool that we use to perform inquiries. The inquiries can be the device ID, name, class or even its clock information. This helps the devices to work in sync.
- hcidump: sniffing of Bluetooth communications is carried out by this tool, it, therefore, gives us a chance to capture data that is being sent over the Bluetooth signal.

The first scanning and reconnaissance step with Bluetooth is to check whether the Bluetooth adapter on the system that we are using is recognized and enabled so we can use it to scan for other devices.

Scanning for Bluetooth Devices with hcitool

Now that we know our adapter is up, we can use another tool in the BlueZ suite called hcitool, which is used to scan for other Bluetooth devices within range.

With the simple scan command, we can find out Bluetooth devices that are transmitting using their discover beacons. That is, the devices set to their

discovery mode. Most of the tools for Bluetooth hacking you are likely to encounter will be using these commands in a script. You should be able to create your tools from these commands using Python script or even bash script.

Using the sdptool to scanning for services

The service discovery protocol, SDP, as it is commonly known, is a protocol of Bluetooth that is used in the searching of Bluetooth services (Bluetooth is a suite of services), and, helpfully, BlueZ provides the sdptool tool for browsing a device for the services it offers. It is also important to note that the device does not have to be in discovery mode to be scanned. The syntax is as follows:

```
sdptool browse MACaddress
```

Seeing Whether the Devices Are Reachable with l2ping

Once we have gathered the MAC addresses of all nearby devices, we can send out pings to these devices, whether they are in discovery mode or not, to see whether they are in reach. This lets us know whether they are active and within range. To send out a ping, we use the l2ping command with the following syntax:

```
l2ping MACaddress
```

Summary

Wireless devices represent the future of connectivity and hacking. Linux has developed specialized commands for scanning and connecting to Wi-Fi APs in the first step toward hacking those systems. The aircrack-ng suite of

wireless hacking tools includes both airmon-ng and airodump-ng, which enable us to scan and gather vital information from in-range wireless devices. The BlueZ suite includes hciconfig, hcitool and other tools capable of scanning and information gathering, which are necessary for hacking the Bluetooth devices within range. It also includes many other tools worth exploring.

Chapter 8: Web Security

Web Security

Just like physical stores, homes, government locations, web applications alongside websites are also susceptible to their security arrangements and protocols being circumvented. What is needed to counter cyber-crimes and the compromising of web applications is robust and reliable security measures.

Web security does this exactly. A functional definition of web security for us can be that it is a set of protocols and protection measures employed in the safeguarding of your website together with your web applications against hacking and against unsanctioned access by personnel who are unauthorized. The integral division of Information Security can protect web services, websites and web applications. This provides crucial security for anything that is carried out on the Internet.

Normally, there exist multiple considerations that are involved when we are dealing with web protection and/or web security. For an application on the web or a website to be said to be secure, it must be backed up by a variety of techniques and checkpoints to guarantee its security. We always have standards of security that need to be adhered to. OWASP is responsible for the highlighting and implementation of these standards. Web developers

who have plenty of experienced normally adhere to OWASP standards and keenly study the Web Hacking Incident Database to be able to know vulnerabilities that lead to websites being hacked and how they are hacked.

Common website security threats

Websites can be attacked in more than one way. Before proceeding, we need to understand some common threats to website security. These are what we shall be looking to avoid and be prepared for during the planning of security measures. Some of these include Spam, Viruses and malware, WHOIS domain registration, and DDoS attacks, among many others.

How to safeguard your website

After getting to know common security threats, let us now focus on how we can prevent them. The assumption that your website is secure is not correct. As long as you have not instituted any safeguard mechanisms, there is a high chance that it can be attacked. Here are a few steps you are required to effect to better the security of your website:

- **Restrict file uploads**

It is risky to let visitors on your website upload files. The uploads may contain a script meant to exploit vulnerabilities present on your website. All uploads need to be treated as a threat to the security of the website.

- **Use HTTPS protocol**

This tells the visitors of a given website that essentially, they are dealing with a proper server. This translates to “no one can intercept the interactions they are having or the content they are viewing.”

- **Secure your personal computer**

Security starts with you! It is important that you take care of the security of your devices. Hackers can use your PC as a gateway to your website. Ensure that you have antivirus software that is updated with the latest definitions. This will protect you from many malicious attacks including from file downloads. It is also possible to inject malware to the websites through stolen FTP login credentials. It is important that you frequently scan your devices for malware and viruses regularly.

- **Change your default CMS settings**

We have seen that numerous attacks are normally automated these days. Malicious users do program bots to help them locate sites still using their default settings. Make it hard for them. Upon installation of a CMS you own, modify the settings which are still on default mode:

Settings required for comments
Controls that users require
Information visibility
Permissions for files

Above are settings you can change right away.

- **Software updates**

All the software must stay up to date. This includes the CMS, plugins, Word Press software, among many others. The updates bring improved functionality, security patches to cover vulnerabilities, fixes for bugs and software glitches, and so on.

- **Select a web hosting plan that is safe**

Web hosting plans that are shared have higher chances of getting compromised. In as much as they are appealing to users due to the potential cost savings, the levels of protection are reduced. As such, they are not a secure option. Remember, cheap is expensive!

- **Limit access to users**

Errors caused by human beings account for a majority of cybersecurity attacks. Reducing or limiting humans can contribute greatly to error reduction. It is not necessary for every employee to access your website. Guests, web designers and consultants likewise, do not deserve automatic access. The least privilege principle needs to be implemented to secure your website.

- **Do a password change**

Password changing is a significant shot in the arm for web security. So, change your password. Changing the password alone is even not enough; make it a habit to change it often.

- **Monitor your security**

You can get utilities that can help you monitor your websites' security online. Such utilities can help you with conducting security audits, which can help to expose potential vulnerabilities. In so doing, you can launch countermeasures before an attack happens.

- **Make a backup for your website**

It is said that when you have been forewarned, you should forearm yourself. It is good to always be prepared for the worse. In this case, the worst that can happen is your website getting compromised. A backup ensures you are at peace since there will be no data that is lost in the event of a compromise.

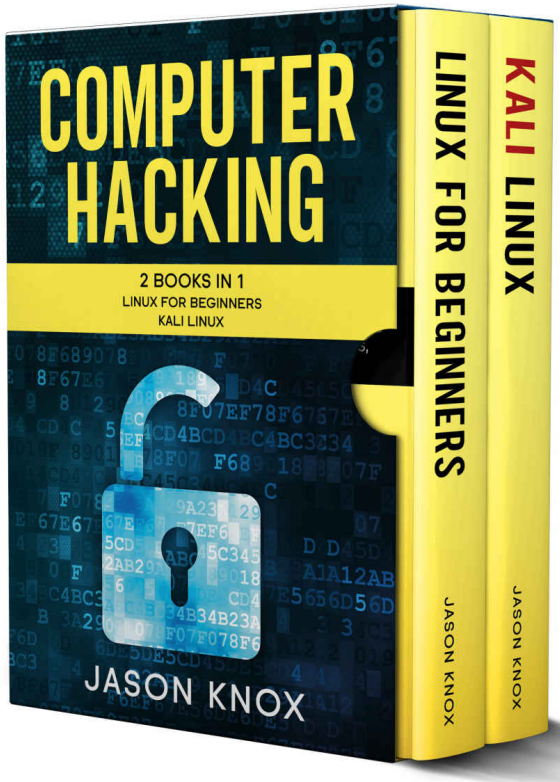
Conclusion

May I take this opportunity to thank you for being able to make it to the end of this informative book, *Kali Linux*. I want to believe that it has been edifying, and through it, you are now able to hit the ground running in matters revolving around hacking. Also, I hope that you have gained the relevant expertise to enable you to begin your hacking career or better your skills if you are already one. I sincerely hope that you have enjoyed turning pages right from the first topic which was Introduction to Kali Linux, all through The Basics of Kali Linux, The Hacking Process, Wireless Network Hacking, Uses and Applications of Kali Linux, Introduction to Cybersecurity, Network Scanning and Management and Web Security. I trust that by studying this book, you have gotten to learn plenty of practical concepts that you need to become a hacking expert.

By now, you must have been able to get access to a vast body of theoretical knowledge regarding the various types of attacks that can be launched on your systems, the reason for launching them and how you are able to safeguard your infrastructure against such attacks. These are your first steps towards becoming a professional hacker. The book covers topical issues like wireless network attacks, cyber-attacks and penetration testing, among others. It, therefore, means that you are now in a good position to discern network attack mechanisms that occur in the real world and prescribe appropriate remedies.

I have also given you a few security measures you can implement to keep your networks safe. The formatting is such that the language is a user-friendly language that you can understand the importance of securing your networks. Going forward, the next step is to put the concepts you have acquired from this book into practice. They say practice makes perfect and it is by practicing that one can become an expert in the field of hacking, more so using Kali Linux. Let the knowledge you have acquired from the book work for you.

Finally, if you found this book useful in any way, a review on Amazon is always welcome!


COMPUTER HACKING
2 BOOKS IN 1
LINUX FOR BEGINNERS
KALI LINUX
JASON KNOX
LINUX FOR BEGINNERS
JASON KNOX
KALI LINUX
JASON KNOX